VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA ÚČETNICTVÍ

Elektronický podpis

Electronic Signature

Student: Bc. Jana Besedová

Vedoucí diplomové práce: Ing. Marcela Palochová, Ph.D.

Ostrava 2011

Místopřísežně prohlašuji, že jsem práci vypracovala samostatně. Přílohy č. 1, č. 2, č. 3 jsem samostatně vypracovala, přílohy č. 4, č. 5, č. 6, č. 7, č. 8, dané mi k dispozici, jsem samostatně doplnila.

Datum: 26. 4. 2011

……

Bc. Jana Besedová

OBSAH

1. Úvod

Informační technologie zasahují do všech oblastí našeho každodenního života a ani oblast autorizace dokumentů se jim nemohla vyhnout. Množství dokumentů v elektronické podobě je značné, riziko padělání narůstá a obvyklý podpis už nestačí.

Podpis neboli signatura je výsledkem uplatnění návyku psaní, vyplývajícího z relativně stálého a individuálního písemného projevu podepisující osoby. Individuálnost písemného projevu je důsledkem vytvoření stereotypu psaní, vypracování složitého systému podmíněných reflexů, které jsou závislé na stupni procvičování. Při vytvoření konkrétního písemného projevu, tedy i podpisu, se uplatňují navíc i aktuální vnější i vnitřní podmínky, na základě kterých může být získaný dynamický stereotyp narušen. Podpis slouží k doložení skutečnosti, že určitá osoba projevila svoji vůli, případně že se v určitou dobu nacházela na určitém místě nebo svým podpisem stvrzuje platnost určitého dokumentu.

Elektronický podpis je číslo. Vstupem pro jeho výpočet je nejen soukromý klíč podepisující osoby, ale i samotný obsah podepisovaného dokumentu. Při sebemenší změně jednou podepsaného dokumentu se změní i toto číslo. Tímto způsobem je zaručena integrita dokumentu. Velikost podepisovaného dokumentu je libovolná, protože jeho obsah je vždy převeden na pevnou velikost. Samotný proces podepisování probíhá automaticky a bez zásahu uživatele. Elektronickým podpisem v digitální podobě je možné podepisovat i ověřovat podpisy rychle a efektivně. Elektronický podpis navíc umožňuje opatřit podpisem i to, co je ručně nemožné – obsah diskety, fotografie nebo přístupy do databáze.

V obou případech, tedy u dokumentu papírového nebo elektronického je rozhodující zachycení obsahu právního úkonu a určení osoby, která právní úkon učinila, tedy zaznamenání informace písemně, na hmotném nosiči trvalým způsobem, umožňujícím tuto informaci předat, získat, vykázat se jí s časovým odstupem, a to případně i jinou osobou, než autorem zápisu.

Elektronický podpis je nezbytnou součástí e-governmentu, jehož cílem je rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu k uživatelům. Pro zabezpečení bezpečné komunikace je v České republice zaveden pojem „kvalifikovaný elektronický podpis“, na základě kterého je možné podepsanou osobu jednoznačně identifikovat.

Cílem diplomové práce je vymezení legislativní úpravy elektronického podpisu v České republice a Evropské unii, poskytnutí základních informací o kryptografii a fungování elektronického podepisování. Práce poskytuje přehled o certifikačních autoritách, obsahuje rovněž podrobné statistiky o poskytovaných službách certifikačních autorit. Praktická část diplomové práce je zaměřena na přehled používaných portálů veřejné správy, názorně analyzuje postup získání a instalace elektronického podpisu a jeho užitím ve vybraných aplikacích. Součástí práce je provedení výzkumu, jehož cílem je mapování rozšíření a využívání elektronického podpisu v podnikatelském sektoru, využívání a spokojenost s aplikacemi e-governmentu. Respondenti měli možnost, kromě hodnocení aplikací, popsat i své praktické zkušenosti s jednotlivými portály veřejné správy.

Metody, které jsou použity v diplomové práci, vycházejí z cíle práce. Základním východiskem diplomové práce je teoretické vymezení základních pojmů. Za metodologický základ lze považovat dialektický přínos, kdy každý jev může být pochopen jako určitá část celku. *Metoda postupu* vychází od jednoduchých kategorií k jejich stále složitějšímu určení, k jejich vzájemným vztahům. *Teoretická a kritická analýza* jsou východiskem pro vymezení dané problematiky, nalezení řešení a specifikace případných nedostatků. *Metoda komparace* byla použita pro porovnání rozsahu a dostupnosti služeb jednotlivých certifikačních autorit, přínosu portálů veřejné správy pro uživatele. Získané poznatky jsou shrnuty pomocí *metody syntézy* a *vědeckého vysvětlení*.

Použité citace nebo převzatá schémata z odborné literatury jsou označeny jako poznámka pod čarou s uvedením jména autora a zdroje čerpání. Obrázky, grafy a kopie obrazovek v diplomové práci jsou vlastním zpracováním, pokud není uvedeno jinak. Vlastní názory, návrhy, stanoviska, doporučení, zhodnocení a dílčí závěry jsou v práci psány zvýrazněnou kurzívou.

2. Legislativní úprava elektronického podpisu v České republice a v Evropské unii

Základním krokem pro elektronickou komunikaci je vytvoření jasných a jednoznačných pravidel pro její fungování. Tato standardizace neprobíhá jen na technologické úrovni, ale nezbytná je i v oblasti užití, práv a povinností spojených s použitím této technologie. Podmínkou nutnou pro využití elektronické komunikace je nastavení takových postupů a principů, které bude možné považovat za rovnocenné běžné papírové komunikaci. Je nezbytné tyto principy zakotvit v obecných a závazných dokumentech a zákonech. Prvním platným zákonem o elektronickém podpisu se stal UTAH Digital Signature act, který vstoupil v platnost už 27. února 1995.

2.1. UNCITRAL – United Nations Commission on International Trade Law

V nadnárodním měřítku se průkopníkem standardizace a legalizace elektronického podpisu stala komise OSN pro mezinárodní právo UNCITRAL – United Nations Commission on International Trade Law,[1] která byla založena Rezolucí VS OSN č. 2205 ze dne 17. prosince 1966. Jejím cílem bylo odstraňovat právní překážky v mezinárodním obchodu a jejím úkolem bylo především podporovat rozvoj, harmonizaci a unifikaci mezinárodního obchodního práva.

UNCITRAL má v současnosti více než 60 členských států a počet členů se stále mění. Členství je strukturováno tak, aby byly zastoupeny všechny regiony i s jejich hospodářskými a právními systémy. Na základě zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, zastřešuje a koordinuje účast České republiky v komisi Ministerstvo průmyslu a obchodu.

Komise UNCITRAL vydává mnoho dokumentů týkajících se mezinárodního obchodu. Pro oblast elektronického podpisu a bezpečné elektronické komunikace jsou nejdůležitější následující dokumenty:

- Doporučení UNCITRAL, týkající se právní závaznosti elektronických údajů (1985);
- Vzorový zákon UNCITRAL o elektronickém obchodu z roku (1996);
- Vzorový zákon o elektronickém podpisu (2001);
- Úmluva o užití elektronických sdělení v mezinárodním obchodě (2005).

[1] Komise OSN pro mezinárodní obchodní právo

Zákonem z roku 1996 připravil UNCITRAL vzorovou právní úpravu umožňující řešení elektronického obchodu a vytvoření prostředí, které zajišťuje rovnocenné postavení pro uživatele písemné i elektronické formy přenosu dat.

Po schválení vzorového zákona o elektronickém obchodu se komise UNCITRAL rozhodla dále věnovat harmonizaci v oblasti elektronického podpisu a poskytování certifikačních služeb a zahájila přípravu příslušných podkladů. Tato činnost byla završena v roce 2001 předložením a schválením vzorového zákona UNCITRAL o elektronickém podpisu.

2.2. Směrnice EU

V Evropě směřoval vývoj ke standardizaci prostředí pro akceptaci bezpečné elektronické komunikace jako alternativy k obecně používané metodě založené na předávání papírových dokumentů. Cílem bylo vytvoření závazné směrnice EU k elektronickému podpisu. V říjnu 1997 byla předložena Evropskému parlamentu studie o zajištění bezpečnosti a důvěryhodnosti elektronické komunikace – směřování k evropským zásadám pro digitální podpisy a šifrování. Výstupním dokumentem je směrnice Evropského parlamentu a Rady 1999/93/ES (dále jen Směrnice) ze dne 13. prosince 1999.

Směrnice se zabývá elektronickými podpisy používanými především pro účely autentizace a aplikací zaručených elektronických podpisů, které mají být právně ekvivalentní klasickým, ručně psaným podpisům. Směrnice se zaměřuje na použitelnost a validitu elektronických podpisů připojených ke konkrétním dokumentům. Stanoví požadavky, které mají být splněny poskytovateli služeb, kteří podporují elektronické podpisy další požadavky vztahující se k podepisující a ověřující straně.

Směrnice byla zpracována tak, aby byly dodrženy tři následující principy:

- Technologická neutralita, kdy se primárně jedná o technologii digitálních podpisů, ale směrnice je otevřena i jiným technologiím;
- Pro poskytovatele certifikačních služeb není primárně definováno žádné schéma pro autorizaci k provádění těchto služeb tak, aby v budoucnu existovala principiální možnost technologických změn;
- Určení zákonné platnosti zaručených elektronických podpisů tak, aby nemohla být popřena jejich platnost pouze na základě toho, že jsou v elektronické podobě.

Dokument Směrnice je poměrně podrobný a zabývá se nejen otázkou definice, tvorby a ověření vlastního elektronického podpisu, ale i otázkou právní uznatelnosti v zemích EU, procesy vydávání certifikátů a dalšími službami poskytovatelů certifikačních služeb a způsoby akreditace.

Právní účinky elektronických podpisů souvisí s akceptací faktu, že elektronický podpis je k datům v elektronické podobě ve stejném vztahu, jako je vlastnoruční podpis k údajům vlastnoručně psaným. S tím souvisí i požadavek na akceptaci dokumentů opatřených zaručeným elektronickým podpisem jako důkazu při případném soudním řízení. Elektronická podoba dokumentů nemá snižovat jejich důvěryhodnost oproti dokumentům papírovým.

Požadavky členských států na elektronický podpis, který je obecně v zemích akceptován jako důvěryhodný, lze rozdělit do pěti základních kategorií.

Kvalifikovaný certifikát splňuje nejpřísnější požadavky na užívání. Pro tvorbu zaručeného elektronického podpisu musí být použito bezpečné zařízení – SSCD (Secure Signature Creation Device) a pro ověření podpisu je užíván kvalifikovaný certifikát. Za bezpečné zařízení pro uživatele elektronického podpisu je považována čipová karta nebo obdobné zařízení splňující příslušné bezpečností a technologické standardy. Jedním z představitelů tohoto výkladu je Slovensko.

Zaručený elektronický podpis založený na kvalifikovaném certifikátu bez hardwarového úložiště je pro klienty jednodušší a levnější variantou. Je méně striktní, ale také méně bezpečný. Legislativa v tomto případě neřeší, jaký nástroj klient pro tvorbu zaručeného elektronického podpisu používá. Požadavkem je pouze užití párových dat spojených s kvalifikovaným certifikátem. Tento přístup je uplatněn v České republice.

Ještě benevolentnější přístup mají země, které netrvají ani na užívání kvalifikovaného certifikátu, uplatňují tedy v podstatě totální liberalizaci bez jakéhokoliv dohledu státního aparátu nad vydáváním a správou certifikátu. Státy jako Irsko a Anglie dokonce mluví o elektronickém podpisu a požadavky na něj nedefinují vůbec. viz [1]

Poslední skupina zemí vyžaduje jen autentizační mechanismus založený na systému jména a hesla a nepovažuje komunikaci s elektronickým podpisem pro komunikaci občana se státní správou za nutnou. (viz Tab. 2.1)

Tab. 2.1: Požadavky členských států EU na kvalifikovaný podpis

Kvalifikovaný podpis uložený na HW úložisti	Kvalifikovaný elektronický podpis	Nedefinovaný certifikát	Nedefinovaný podpis	Autentizace
Belgie	Bulharsko	Dánsko	Anglie	Kypr
Itálie	Chorvatsko	Lucembursko	Irsko	
Lotyšsko	Česká republika	Polsko		
Portugalsko	Estonsko			
Slovensko	Finsko			
Španělsko	Francie			
Švédsko	Maďarsko			
Rakousko	Malta			
	Německo			
	Nizozemí			
	Rumunsko			
	Řecko			
	Slovinsko			
	Turecko			

Zdroj: Study for the European commission – The legal and market aspects of electronic signatures

Transformace požadavků Směrnice do právních norem jednotlivých států byla realizována několika způsoby. Nejrozšířenějším je vydání zákona o elektronickém podpisu jako samostatné právní normy. Druhým způsobem je komplexní přístup se zapracováním dopadů direktivy do všech relevantních dokumentů. Třetím, nejméně rozšířeným přístupem, je úprava právních norem podle potřeby v jednotlivých oblastech. (viz Tab. 2.2)

Tab. 2.2: Postup transformace Směrnice do právních norem členských států EU

Samostatný zákon	Komplexní přístup	Jednotlivé oblasti	Podle potřeby
Belgie	Rakousko	Malta	Bulharsko
Česká republika	Německo	Irsko	Anglie
Dánsko	Itálie		
Estonsko	Portugalsko		
Finsko	Slovinsko		
Francie	Španělsko		
Kypr	Turecko		
Litva			
Lotyšsko			
Lucembursko			
Maďarsko			
Nizozemí			
Polsko			

Samostatný zákon	Komplexní přístup	Jednotlivé oblasti	Podle potřeby
Rumunsko			
Řecko			
Slovensko			
Švédsko			

Zdroj: Study for the European commission – The legal and market aspects of electronic signatures

2.3. Zákon o elektronickém podpisu

Dne 29. 6. 2000 byl ve Sbírce zákonů, částce 68 zveřejněn zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (dále Zákon o elektronickém podpisu). Zákon o elektronickém podpisu byl dále novelizován, naposledy pak zákonem č. 227/2009 Sb., zákonem č. 281/2009 Sb. a zákonem č. 101/2010 Sb. Smyslem Zákona o elektronickém podpisu je umožnit použití digitálního podpisu v rámci elektronické komunikace jako ekvivalent podpisu vlastnoručního při běžné listinné formě komunikace. Zákon o elektronickém podpisu byl vytvořen na základě směrnice Evropské unie 1999/93/EC ze dne 13. 12. 1999.

Dne 26. července 2004 nabyla účinnosti novela zákona o elektronickém podpisu (č. 440/2004 Sb.). Tento předpis nově zavádí pojem kvalifikované časové razítko, které prokazuje existenci elektronického dokumentu v čase. Další změnou je možnost používat elektronické značky. Pro ty se stejně jako pro zaručený elektronický podpis používá technologie digitálních podpisů. Rozdíl mezi nimi spočívá v tom, že elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy.

Dne 15. dubna 2010 nabyla účinnosti novela Zákona o elektronickém podpisu. Tento předpis přidává Ministerstvu vnitra povinnost vést a zveřejňovat seznam důvěryhodných certifikačních služeb a stanoví orgánům veřejné moci povinnost uznávat kvalifikované certifikáty vydané v ostatních členských státech EU.

2.3.1. Klíčové pojmy Zákona o elektronickém podpisu[2]

Pro účely zákona se rozumí

a) **elektronickým podpisem** údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují ověření totožnosti podepsané osoby k datové zprávě,

[2] Zákon č. 227/2000 Sb., o elektronickém podpisu, § 2

b) **zaručeným elektronickým podpisem** elektronický podpis, který splňuje následující požadavky:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

c) **datovou zprávou** elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,

d) **podepisující osobou** fyzická osoba, která má prostředek pro vytváření podpisu a jedná jménem svým nebo v zastoupení jiné fyzické nebo právnické osoby,

e) **poskytovatelem certifikačních služeb** subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

f) **akreditovaným poskytovatelem certifikačních služeb** poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,

g) **certifikátem** datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost,

h) **kvalifikovaným certifikátem** certifikát, který má náležitosti stanovené tímto zákonem a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty.

Podle Zákona o elektronickém podpisu je příjemce zprávy povinen učinit veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

Popis těchto úkonů, vedoucích k ověření platnosti zaručeného elektronického podpisu uvádí příloha vyhlášky č. 496/2004 sb., o elektronických podatelnách:

1. Ověření zaručeného elektronického podpisu a elektronické značky

Ověření podpisu podepisující osoby nebo elektronické značky označující osoby datové zprávy se provádí podle standardů asymetrických kryptografických algoritmů a kryptografických hashovacích funkcí odpovídajících schématům použitým při vytváření zaručeného elektronického podpisu. Ověření se provádí pomocí aplikace bez zásahu ověřující osoby.

2. Ověření platnosti certifikátu

a) Ověření intervalu doby platnosti

Ověření, zda v době doručení datové zprávy byl kvalifikovaný certifikát podepisující osoby nebo kvalifikovaný systémový certifikát označující osoby v intervalu doby platnosti. Ověření se provádí bez zásahu ověřující osoby.

b) Ověření elektronické značky certifikátu

c) Ověření, zda certifikát nebyl zneplatněn

Rozhodným seznamem zneplatněných certifikátu je pro tyto účely seznam, jehož platnost začíná bezprostředně po čase doručení datové zprávy. Ověření provádí ověřující osoba, aplikace jej zpravidla neprovádí.

d) Ověření elektronické značky seznamu zneplatněných certifikátů

e) Certifikační cesta

Elektronická značka kvalifikovaného certifikátu podepisující osoby nebo kvalifikovaného systémového certifikátu označující osoby je založena na kvalifikovaném systémovém certifikátu poskytovatele. I ten může být označen elektronickou značkou poskytovatele, která je založena na dalším kvalifikovaném systémovém certifikátu poskytovatele. Tento vztah mezi certifikáty se označuje pojmem certifikační cesta. Pro ověření platnosti certifikátu je nutné provést ověření platnosti všech certifikátů v certifikační cestě podle písmene a) až d) tohoto bodu. Certifikační cesta je vyznačena v každém vydaném certifikátu.

3. Ověření kvalifikovaného časového razítka

Provádí se stejně jako ověření zaručeného elektronického podpisu.

2.3.2. Povinnosti poskytovatelů certifikačních služeb[3]

Poskytovatelé certifikačních služeb jsou povinni:

- zajistit, aby certifikáty jimi vydané jako kvalifikované obsahovaly všechny náležitosti kvalifikovaných certifikátů stanovené Zákonem o elektronickém podpisu,
- zajistit, aby údaje uvedené v kvalifikovaných certifikátech byly přesné, pravdivé a úplné,
- před vydáním certifikátu bezpečně ověřit odpovídajícími prostředky totožnost osoby, které kvalifikovaný certifikát vydává,
- zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů a seznamu zneplatněných certifikátů,
- přijímat do pracovního poměru osoby, které mají odborné znalosti, zkušenosti a kvalifikaci nezbytnou pro poskytované služby,
- používat bezpečné systémy a nástroje elektronického podpisu a zajistit bezpečnost postupů, které tyto systémy a nástroje podporují,
- přijmout odpovídající opatření proti zneužití a padělání kvalifikovaných certifikátů,
- mít k dispozici dostatečné finanční zdroje v souladu s požadavky tohoto zákona a s ohledem na riziko odpovědnosti za škody,
- uchovávat veškeré informace a dokumentaci po dobu nejméně 10 let od ukončení platnosti kvalifikovaného certifikátu,
- před uzavřením smluvního vztahu s osobou, která o certifikát žádá, informovat ji písemně o přesných podmínkách používání kvalifikovaného certifikátu,
- používat bezpečný systém pro uchování kvalifikovaných certifikátů.

[3] Zákon č. 227/2000 Sb., o elektronickém podpisu, § 6, odst. 1

O veškeré činnosti poskytované certifikačních služeb musí být vedena provozní dokumentace, která musí obsahovat tyto údaje:

a) smlouvu s podepisující osobou o vydání kvalifikovaného certifikátu,
b) vydaný kvalifikovaný certifikát,
c) kopie předložených osobních dokladů podepisující osoby,
d) potvrzení o převzetí kvalifikovaného certifikátu podepisující osobou,
e) přesné časové určení doby platnosti vydaného kvalifikovaného certifikátu.

2.4. Náležitosti kvalifikovaného certifikátu[4]

Kvalifikovaný certifikát musí obsahovat:

- označení, že je vydán jako kvalifikovaný certifikát;
- obchodní jméno poskytovatele certifikačních služeb a jeho sídlo;
- jméno a příjmení podepisující osoby;
- zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu;
- data pro ověřování podpisu;
- zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává;
- číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb;
- počátek a konec platnosti kvalifikovaného certifikátu;
- údaje o tom, zda se používání certifikátu omezuje podle povahy a rozsahu jen pro určité použití, případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

2.5. Certifikační politiky

Kvalifikované certifikáty se řídí náležitostmi danými zákonem o elektronickém podpisu. To platí i pro účely, ke kterým jsou kvalifikované certifikáty využívány. V případě kvalifikovaným certifikátů se jedná pouze o podepisování dokumentů. Zákon definuje pouze základní požadavky na kvalifikované certifikáty, jako je např. jméno a příjmení podepisované osoby, jméno a označení vydavatele. Řada dalších vlastností a postupů v zákoně uvedena není a je zcela na rozhodnutí certifikačních autorit, jak budou postupovat. Sami tak rozhodují například o tom, jaké dokumenty budou požadovat pro ověření totožnosti, jaká bude doba platnosti certifikátu.

[4] Zákon č. 227/2000 Sb., o elektronickém podpisu, § 12, odst. 1

Všechna tato rozhodnutí jsou součástí certifikačních politik. Tyto certifikační politiky jsou dokumenty, ve kterých poskytovatelé přesně a detailně popisují podmínky a postupy při vydávání certifikátů, možnosti a způsoby jejich využití nebo například možnosti revokace certifikátů.

Certifikační politiky jsou odlišné pro různé druhy certifikátů:[5]

Kořenová certifikační autorita PostSignum (PostSignum Root QCA) má jednu certifikační politiku, podle které vydává kvalifikované certifikáty svým podřízeným certifikačním autoritám.

Kvalifikovaná certifikační autorita PostSignum (PostSignum QCA, podřízená kořenové certifikační autoritě) má dvě certifikační politiky, jednu pro vydávání kvalifikovaných osobních certifikátů a jednu pro vydávání kvalifikovaných systémových certifikátů.

Komerční certifikační autorita PostSignum (PostSignum VCA, podřízená kořenové CA) má tři certifikační politiky, jednu pro vydávání komerčních osobních certifikátů, jednu pro vydávání komerčních serverových certifikátů, a jednu pro vydávání certifikátů pro šifrování.

Každý zákazník, kterému je vydáván certifikát, musí být seznámen s příslušnou certifikační politikou, a následně potvrdit podpisem na smlouvě o vydání certifikátu, že s certifikační politikou souhlasí. Je to nutné proto, že v certifikační politice jsou definovány základní vztahy mezi poskytovatelem certifikačních služeb a zákazníkem.

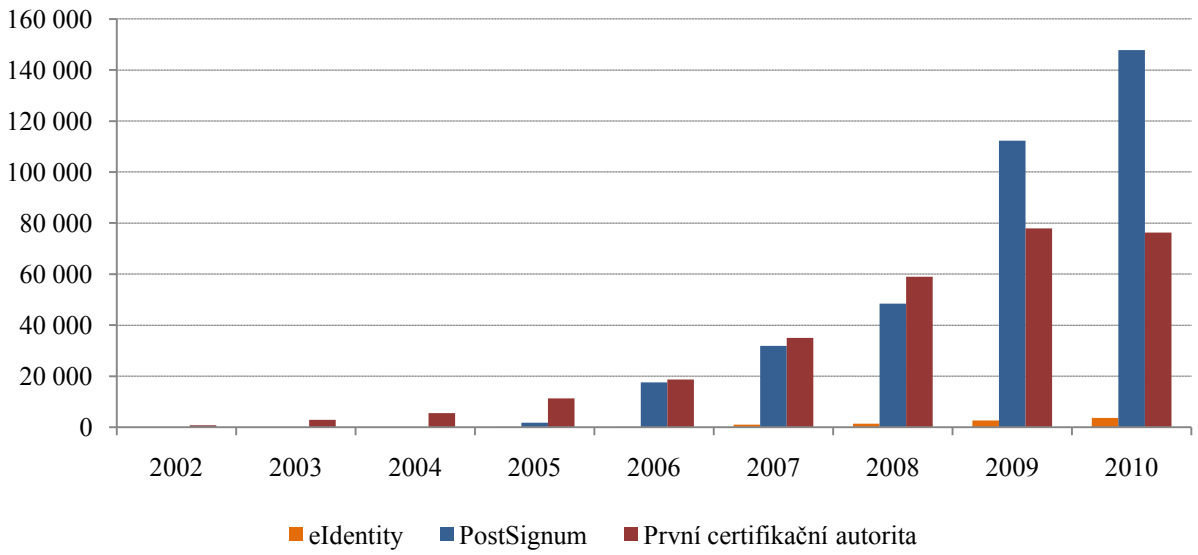
[5] Vzorový seznam jednotlivých certifikačních politik certifikační autority PostSignum dostupný z www.postsignum.cz

Tab. 2.3: Přehled akreditovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb v České republice k 31. 3. 2011

POSKYTOVATELÉ CERTIFIKAČNÍCH SLUŽEB	KVALIFIKOVANÉ SLUŽBY	ZAHÁJENÍ VYDÁVÁNÍ
První certifikační autorita, a. s.	Vydávání kvalifikovaných certifikátů	březen 02
IČO 26 43 93 95	Vydávání kvalifikovaných systémových certifikátů	únor 06
Podvinný mlýn 2178/6	Vydávání kvalifikovaných časových razítek	únor 06
PSČ 190 00 Praha 9		
Česká pošta, s. p.	Vydávání kvalifikovaných certifikátů	září 05
IČO 47 11 49 83	Vydávání kvalifikovaných systémových certifikátů	duben 05
Olšanská 38/9	Vydávání kvalifikovaných časových razítek	červenec 09
PSČ 225 99 Praha 3		
eIdentity a. s.	Vydávání kvalifikovaných certifikátů	srpen 05
IČO 27 11 24 89	Vydávání kvalifikovaných systémových certifikátů	srpen 05
Vinohradská 184/2396	Vydávání kvalifikovaných časových razítek	srpen 10
PSČ 130 00 Praha 3		

Zdroj: http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb-320051.aspx

Graf 2.1: Počet vydaných kvalifikovaných certifikátů v letech 2002 – 2010



Zdroj: Česká pošta, s.p., (detail viz příloha)

3. Technologie elektronického podpisu

Elektronická komunikace se stala běžnou součástí každodenního života a pro ochranu přenášených dat je nezbytné zajistit jejich důvěryhodnost a bezpečnost ve stejné míře jako při osobním styku. Tento aspekt nabývá ještě výraznější důležitosti v rámci komunikaci ve sféře státní správy, financí a zdravotnictví.

Základními bezpečnostními cíli, jejichž splnění by měl důvěryhodný systém zabezpečit, jsou:

- důvěrnost informací – systém musí zabezpečit, aby k informacím měly přístup pouze osoby, kterým jsou určeny;
- integrita – systém musí být zajištěn proti změně přenášených dat;
- nepopiratelnost – systém musí mít schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, vlastnictví, odeslání, případně přijetí zprávy.

Ochrana přenášených dat je prováděna na dvou úrovních. První oblastí ochrany dat je jejich ochrana u správce nebo uživatele. Další oblastí je ochrana dat při jejich přenosu sítí. Přenosové trasy jsou natolik rozsáhlé, že je není možné fyzicky zabezpečit po celé jejich délce. Pro zabezpečení citlivých dat při přenosu je tedy nezbytné použít šifrování.

Kvalita ochrany zprávy je dána použitou šifrovací metodou. V zásadě rozlišujeme dvě šifrovací metody – symetrickou kryptografii a asymetrickou kryptografii, kterou zahrnujeme do kryptografie s veřejným klíčem. viz [1]

3.1. Symetrická kryptografie

Symetrická kryptografie se vyznačuje použitím jednoho šifrovacího klíče. To znamená, že je stejný klíč použitý pro zašifrování zprávy na straně odesilatele i pro dešifrování zprávy na straně příjemce. Z této skutečnosti vyplývá nutnost před začátkem komunikace předat šifrovací klíč druhé straně. Při použití symetrické kryptografie je možné zabezpečit důvěrnost transakcí, ale stěžejní nevýhodou je obtížná distribuce šifrovacích klíčů v rozsáhlých sítích. viz [2]

3.2. Asymetrická kryptografie

Asymetrické šifry nepoužívají jeden tajný šifrovací klíč sdílený mezi odesílatelem a příjemcem, ale vždy se používá pár šifrovacích klíčů. Jeden klíč pro šifrování a druhý pro dešifrování. U digitálního podpisu jsou u některých šifer operace šifrování a dešifrování zaměnitelné, proto se nejedná o šifrovací a dešifrovací klíč, ale o veřejný a soukromý klíč.

Princip kryptografie s veřejným klíčem spočívá v tom, že data šifrovaná jedním z klíčů lze dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Soukromý klíč je s maximální možnou mírou chráněn majitelem, zatímco druhý veřejný klíč je zveřejněn. Byla-li zpráva šifrována soukromým klíčem a příjemce zprávy má k dispozici odpovídající veřejný klíč, kterým zprávu lze dešifrovat, zná odesílatele. Protože je veřejný klíč znám všem, nelze soukromým klíčem šifrovanou zprávu považovat za zašifrovanou, ale pouze za autorizovanou. Toto je principem elektronického podpisu. viz [2]

Tímto způsobem je vyřešena integrita dat a nepopiratelnost na straně odesílatele. Jestliže navíc příjemce pošle autorizované potvrzení o doručení, je zajištěna nepopiratelnost i na straně příjemce. Tento postup však neřeší požadavek důvěrnosti zpráv, protože pomocí veřejného klíče odesílatele si ji může přečíst každý, kdo ji získá. Pro zajištění důvěrnosti zpráv je třeba využít šifrování pomocí veřejného klíče adresáta. Při takovém zašifrování máme jistotu, že ji přečte pouze adresát se svým soukromým klíčem.

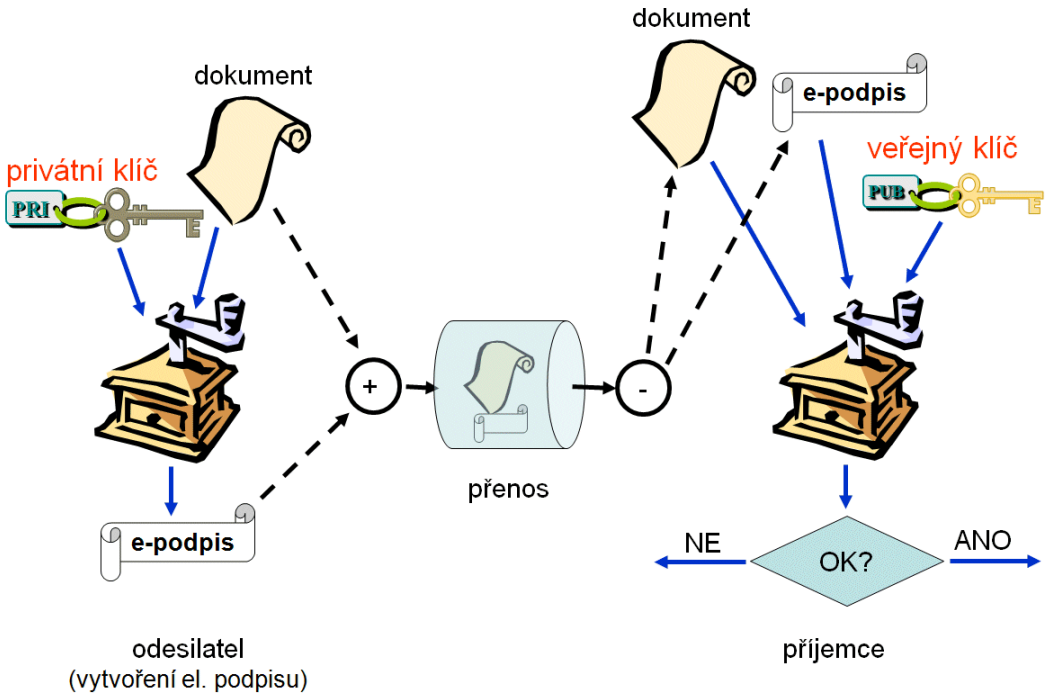
Systém pro šifrování a podepisování zpráv pomocí asymetrické kryptografie tedy pracuje tímto způsobem:

1. Zpráva je na straně odesílatele autorizována (podepsána) s využitím soukromého klíče odesílatele, autorizován je čitelný text zprávy.

2. Následně je podepsaná zpráva pomocí veřejného klíče příjemce zašifrována.

3. Na straně příjemce je zpráva nejprve dešifrována soukromým klíčem příjemce. Tímto je zajištěna adresnost zprávy, a teprve poté je pomocí veřejného klíče odesílatele ověřena identita odesílatele a současně je získán čitelný text zprávy.

Obr. 3.1: Podpis elektronického dokumentu



Zdroj: http://www.lupa.cz/clanky/datove-schranky-pracujeme-snbspepodpisy-v/

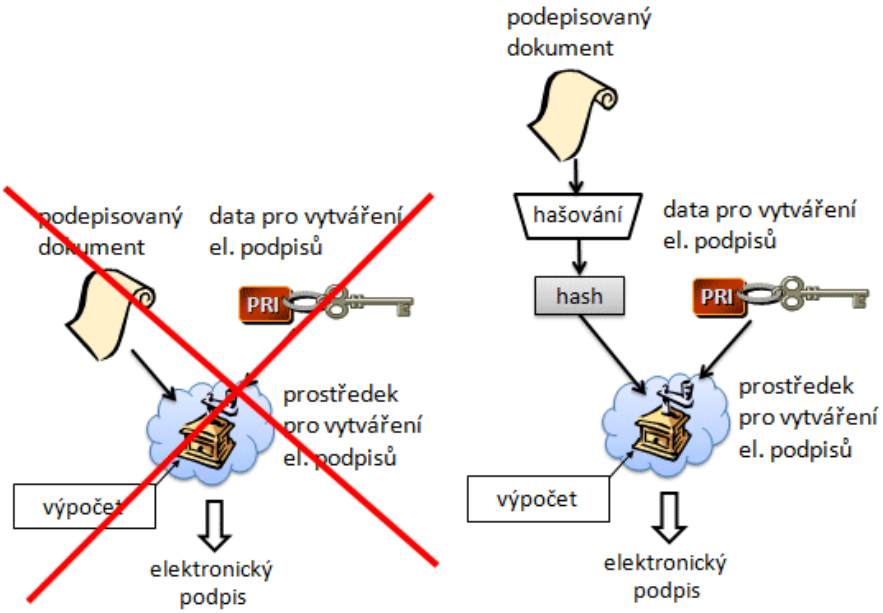
Pokud není možné pozitivně ověřit platnost e-podpisu na doručeném dokumentu, je to způsobeno tím, že příjemce použil pro otevření nesprávný certifikát nebo byl dokument či podpis cestou změněn. Aby se zabránilo ověřování dokumentu nesprávným certifikátem, přikládá se k elektronicky podepsanému dokumentu i použitý podpisový certifikát. Většina nástrojů pro tvorbu elektronického podpisu to standardně udělá za odesílatele.

3.3. Hash a hashovaní funkce

Metody a algoritmy, které se používají při podepisování dokumentů, pracují pouze s bloky dat o pevné velikosti. Tyto bloky dat musí být dostatečně malé, aby jejich zpracování bylo dostatečně rychlé. Při hashování dochází k převodu dokumentu z libovolně velkého na dokument o pevně dané velikosti. Hashování probíhá tak, že se z dokumentu o libovolné velikosti vytvoří otisk o pevně dané velikosti. Od roku 2010 je doporučovanou hashovaní funkcí SHA-2, která pracuje s otisky o velikosti 224, 256, 384 nebo 512 bitů. Vytvoření otisku je zabudováno do procesu podepisování a probíhá automaticky bez zásahu uživatele.

Výpočet hash hodnoty zprávy je velmi rychlý. Nejprve se při podpisu zprávy vypočte hash hodnota zprávy, která bývá výrazně kratší než podepisovaná zpráva, a ta se zašifruje některým asymetrickým algoritmem s použitím soukromého klíče. Výsledkem je elektronický podpis. Ten je potom odeslán jako příloha zprávy nebo v samostatném bloku. Výhodou elektronického podpisu je, že splňuje stejná bezpečnostní kritéria jako autorizace celého dokumentu, provedení však trvá nesrovnatelně kratší dobu. Kontrola elektronického podpisu zprávy u příjemce probíhá tak, že ke zprávě je příjemcem podle stejného algoritmu spočítána nová hash hodnota a ta je potom srovnávána s dešifrovanou hash hodnotou obsaženou v dodatku zprávy. Obě hodnoty si musí být rovny. Pokud tomu tak není, nepovažuje se elektronický podpis za platný a zpráva za důvěryhodnou. viz [10]

Obr. 3.2: Hashování



Zdroj: PETERKA, J. Báječný svět elektronického podpisu [online]. 2011, [cit. 2011-03-12]. Dostupný z WWW: <http://www.bajecnysvet.cz>.

Nejproblematičtější oblastí bezpečné komunikace je správa a uchování kryptografických klíčů. Při použití symetrické kryptografie je třeba maximálně zabezpečit jednotlivé šifrovací klíče společně se seznamem příslušných partnerů. Vzhledem k nutnosti poměrně časté změny klíče kvůli souvislosti s možným prolomením šifer, dochází k ohrožení bezpečnosti a zajištění ochrany je finančně nákladné a logisticky náročné.

Při užití asymetrické kryptografie je situace jednodušší. Nestačí však chránit pouze soukromý klíč. Je nutné zabezpečit i ochranu veřejných klíčů všech komunikujících účastníků, a k nim jejich jednoznačnou identifikaci. Při velkém počtu komunikujících subjektů je tato otázka jednou z nejdůležitějších. Uchování těchto informací se tak stává nejslabším článkem bezpečné komunikace.

Řešením problému správy, distribuce a uchování klíčů je využití takzvaného certifikátu. Certifikát lze chápat jako obdobu průkazu totožnosti.

Certifikáty obsahují veřejný klíč, jméno a další údaje, které zajišťují identifikaci subjektu, kterému je certifikát vydán. Obsahují též datum počátku platnosti, datum ukončení platnosti, jméno certifikační autority, která certifikát vydala, sériové číslo a další informace.

Poskytovatelem certifikátů je certifikační autorita. Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako třetí, nezávislý a důvěryhodný subjekt, který prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu s jeho dvojicí klíčů a následně s jeho elektronickým podpisem. Certifikační autorita garantuje jedinečnost subjektů podle užité identifikace subjektu v rámci vydávaných certifikátů. To je zajištěno legislativními a technickými pravidly provozu instituce certifikačních autorit. Splnění těchto požadavků potvrdí certifikační autorita podpisem dokumentu svým soukromým klíčem a následným vydáním certifikátu.

Certifikát je podepsaným dokumentem se všemi důsledky z toho plynoucími, tedy zejména autorizace a integrita dat. Certifikační autorita je garantem pravosti certifikátu a není možné měnit ani upravit fyzickou ani elektronickou identitu vlastníka certifikátu. Tím, že certifikační autorita zaručuje správnost vydaného certifikátu, odstraňuje nutnost smluvní důvěryhodné výměny klíčů mezi dvěma subjekty navzájem a jejich dohoda spočívá pouze v domluvě o společně uznávané certifikační autoritě. Certifikační autorita umožňuje bezpečnou komunikaci i subjektům, které se navzájem nikdy nepotkali a nevyměnili si navzájem své klíče. viz [10]

3.4. Typy certifikátů

Kvalifikovaný certifikát nesmí být vystaven neexistující fyzické osobě. Jestliže je tedy vydán kvalifikovaný certifikát, patří pouze existujícímu subjektu. Vzhledem k zavedení elektronických značek a časových razítek je možné vydat kvalifikovaný certifikát i jiným subjektům, právnickým osobám, organizačním složkám státu a podobně.

Aby se rozlišily certifikáty pro fyzické osoby a ostatní subjekty, bylo zavedeno rozdělení na **kvalifikované osobní certifikáty** určené pouze existujícím fyzickým osobám a **kvalifikované systémové certifikáty** určené fyzickým osobám podnikajícím i nepodnikajícím a právnickým osobám.

Správným rozlišujícím kritériem mezi osobními a systémovými kvalifikovanými certifikáty je jejich účel. Osobní certifikáty se používají v souvislosti s elektronickými podpisy a systémové se používají v souvislosti s elektronickými značkami a časovými razítky. U obou variant kvalifikovaných certifikátů ale platí, že požadavky na ně definuje zákon. Ten předepisuje jejich vydavateli velmi důkladně identifikovat subjekt, kterému kvalifikovaný certifikát vystavuje. Jak konkrétně vydavatel tento požadavek realizuje, už je specifikováno v příslušné certifikační politice.

Všechny ostatní certifikáty se označují jako komerční certifikáty. **Komerční osobní certifikáty** jsou vystavovány pouze fyzickým osobám a mohou být použity pro šifrování, autentizaci i podepisování. **Komerční serverové certifikáty** mohou být vystavovány fyzickým osobám i právnickým a používají se zejména pro identifikaci a autentizaci webových serverů vůči jejich klientům, a pro zabezpečenou komunikaci mezi klienty a servery. Některé certifikační autority nabízejí **komerční šifrovací certifikáty**, které jsou určeny pouze pro šifrování.

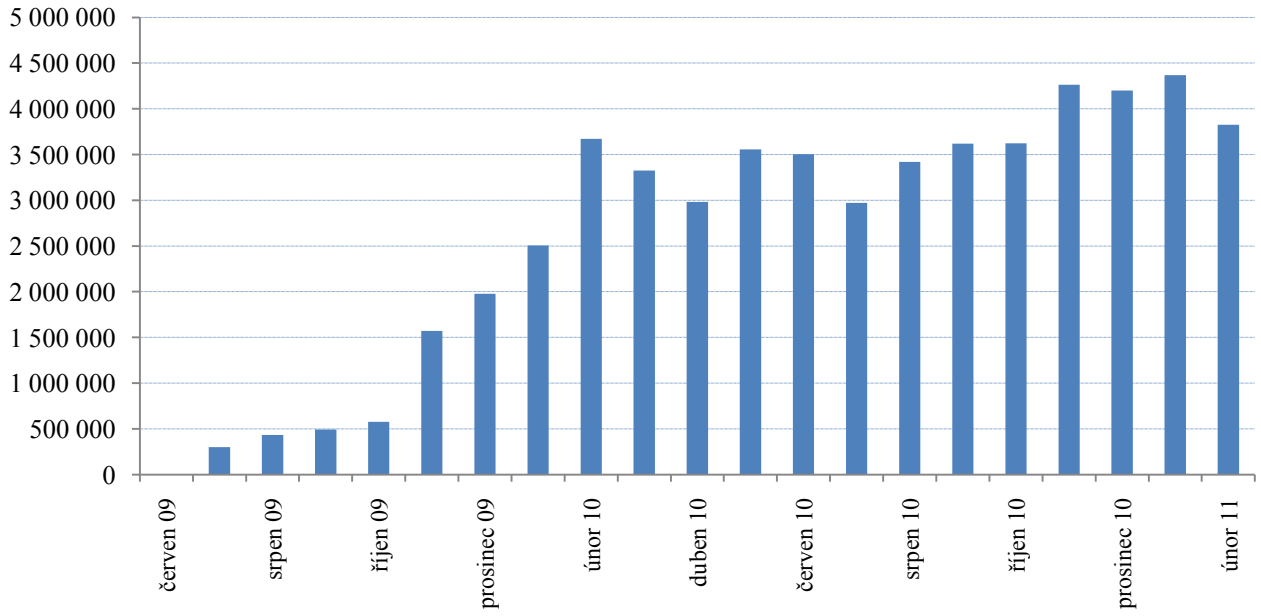
3.5. Elektronická značka a časové razítko

Novelou zákona č. 227/2000 Sb. zákonem č. 440/2004 Sb. byl do našeho právního řádu zaveden pojem elektronická značka a časové razítko. Elektronické značky jsou založeny na systémových certifikátech, a proto mohou být vystaveny i právnickým osobám. Evropské směrnice pojem systémové certifikáty neznají, a proto je zavedení elektronických značek v České republice unikátní.

Časový údaj o době vzniku elektronického podpisu je jeho součástí, ale protože jeho zdrojem je systémový čas počítače, nedá se na tento údaj zcela spoléhat. Časové razítko vzniká tak, že uživatel z něj vytvoří otisk, který pošle poskytovateli časových razítek. Ta otisk podepíše s uvedení časového údaje, kdy se tak stalo a vrátí jej uživateli. Poskytovatel časového razítka nenese odpovědnost za obsah podepsaného a časovým razítkem opatřeného dokumentu. Podobně jako notář, který se nevyjadřuje k obsahu dokumentu, u kterého ověřuje podepisující osobu.

Časové razítko neříká, jak dlouho před ním označený dokument existoval. Podstatná je skutečnost, že existoval v okamžiku, kdy je časovým razítkem označen a poskytovatel za toto ručí.

Graf 3.1: Vydaná časová razítka PostSignum (v ks)



Zdroj: Česká pošta s.p., (detail viz příloha)

3.6. Certifikační autorita

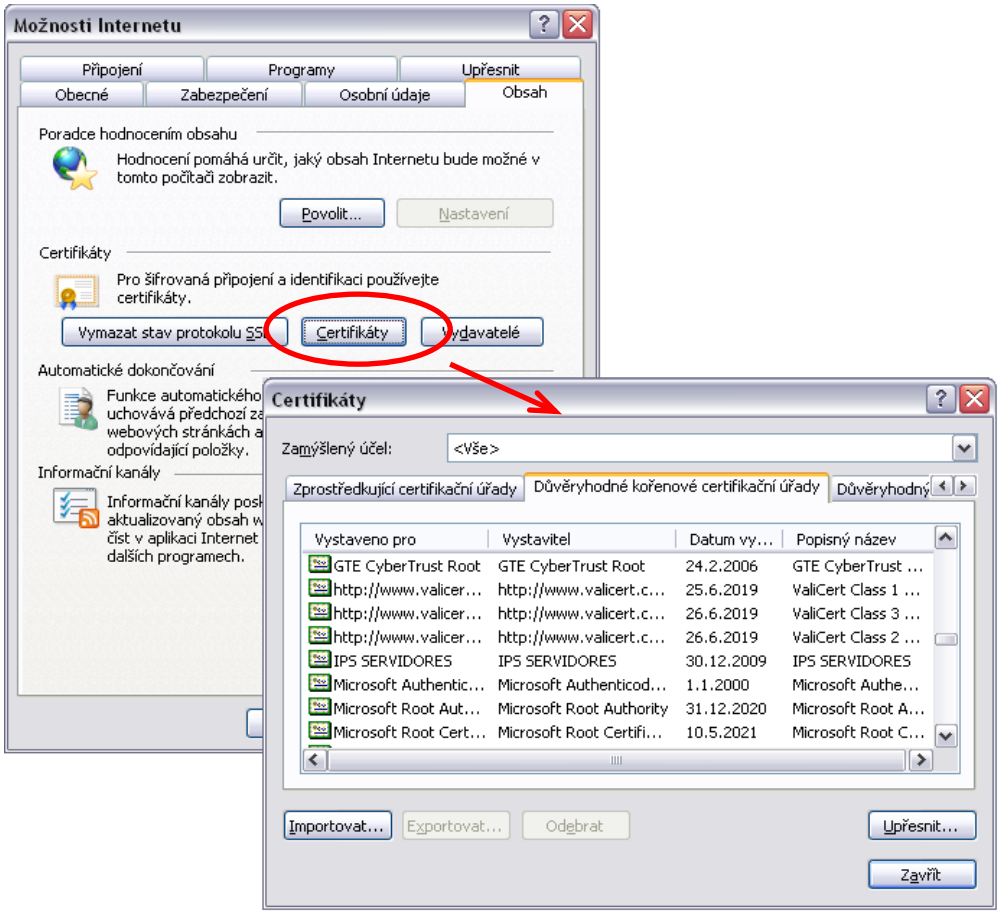
Za důvěryhodnost certifikátu ručí jeho vydavatel, certifikační autorita. Aby bylo možné ověřit, že certifikát vydala předpokládaná certifikační autorita, je nutné získat její certifikát, který obsahuje data pro ověření elektronického podpisu certifikační autority. MS Windows certifikáty poskytovatelů certifikačních služeb v souvislosti s jejich funkcí a zařazením rozděluje do tří kategorií:

- Implicitní kořenové certifikační autority,
- Zprostředkující certifikační autority,
- Důvěryhodní vydavatelé.

3.6.1. Implicitní kořenové certifikační autority

Implicitně důvěryhodné certifikační autority jsou po instalaci systému do počítače přístupné přes záložku Nástroje internetového prohlížeče a položku Možnosti internetu.

Obr. 3.3: Seznam implicitních důvěryhodných kořenových certifikačních úřadů



3.6.2. Zprostředkující certifikační autority

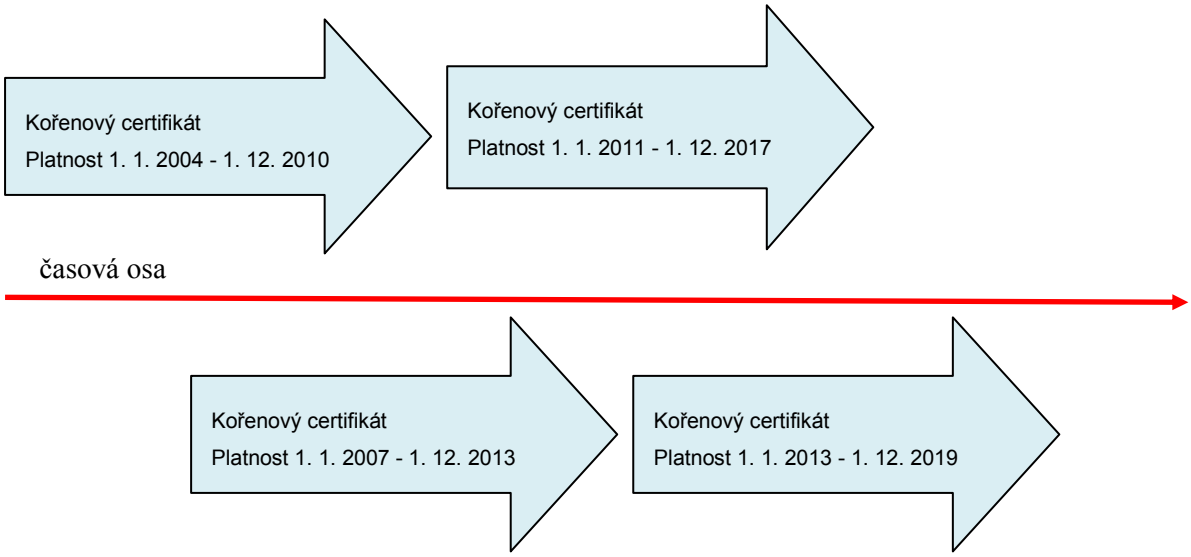
Certifikát je vydán vyšší, nadřízenou institucí, o jejíž důvěryhodnosti se již nepochybuje a je zmocněna zvláštním zákonem. Na Slovensku vydává takové certifikáty Certifikační autorita Národný bezpečnostný úrad v souladu se zákonem o elektronickém podpisu Slovenské republiky.

3.6.3. Důvěryhodní vydavatelé

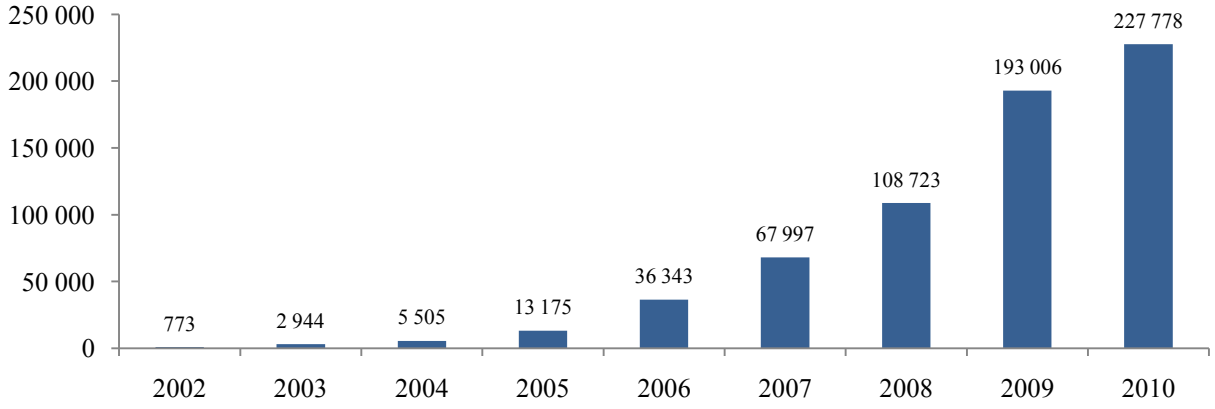
Způsobem, který je běžnější a je zavedený v České republice je ten, že si certifikační autorita vydá certifikát sama. Jedná se tedy o certifikát, kdy je vystavitel i vlastník certifikátu stejný. Tento typ certifikátů, označovaný jako kořenový, sám o sobě v žádném případě neposkytuje dostatečnou záruku pravosti a důvěryhodnosti vydavatele. Tu je třeba získat předáním certifikátu komunikujícím stranám důvěryhodným způsobem nebo zveřejněním takového certifikátu prostřednictvím důvěryhodného prostředníka.

Platnost certifikátu CA není neomezená. I když je platnost delší a zpravidla trvá 5 let, i tento certifikát po určité době vyprší. Při ověřování platnosti a důvěryhodnosti klientského certifikátu se postupuje tak, že v jednom z prvních kroků se kontroluje platnost podpisu CA na klientském certifikátu podle dat (veřejného klíče) uvedených v certifikátu vydavatele. Proto musí být v době ověřování platnosti klientského certifikátu platný i certifikát CA. Aby nedošlo v žádném okamžiku k vypršení platnosti certifikátu CA, mají certifikáty CA souběžně platné dva i více certifikátů.

Graf 3.2: Souběžná platnost certifikátů CA



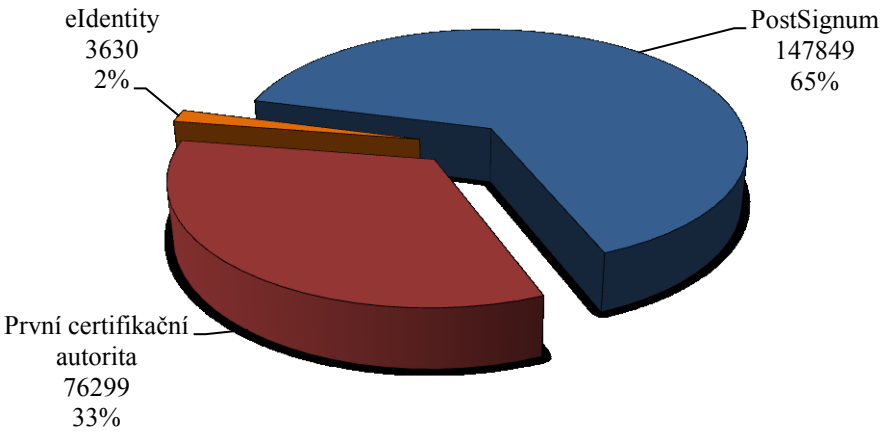
Graf 3.3: Počet vydaných kvalifikovaných certifikátů v letech 2002 – 2010 v České republice



Zdroj: Data poskytnutá certifikačními autoritami, (detail viz příloha)

V roce 2002 vydala první akreditovaná certifikační autorita prvních 773 certifikátů, v roce 2005 začala vydávat kvalifikované certifikáty Česká pošta s.p. Třetí akreditovaná společnost v České republice eIdentity a.s. má zanedbatelný podíl na tomto trhu.

Graf 3.4: Podíl CA na trhu certifikátů v roce 2010



Zdroj: Data poskytnutá certifikačními autoritami, (detail viz příloha)

Tab. 3.1: Ceník certifikátů jednotlivých certifikačních autorit platný k 31. 3. 2011 (v Kč)

Typ certifikátu	První certifikační autorita a.s.	Certifikační služba PostSignum	eIdentity a.s.
Kvalifikovaný certifikát	495	396	474
Kvalifikovaný systémový certifikát	780	1788	3480
Komerční osobní certifikát	395	348	354
Komerční serverový certifikát	1170	800	1074

Zdroj: www.ica.cz, www.postsignum.cz, www.eidentity.cz,

Tab. 3.2: Síť poboček certifikačních autorit

Kraj	První certifikační autorita a.s.	Certifikační služba PostSignum	eIdentity a.s.
Jihočeský	1	83	0
Jihomoravský	2	118	0
Karlovarský	1	32	0
Královéhradecký	1	59	0
Liberecký	1	44	0
Moravskoslezský	3	114	0
Olomoucký	2	57	0
Pardubický	2	50	0
Plzeňský	2	53	0
Praha	3	100	4
Středočeský	3	95	0
Ústecký	3	64	0
Vysočina	2	46	0
Zlínský	2	53	0
Celkový počet poboček	28	968	4

Zdroj: www.ica.cz, www.postsignum.cz, www.eidentity.cz

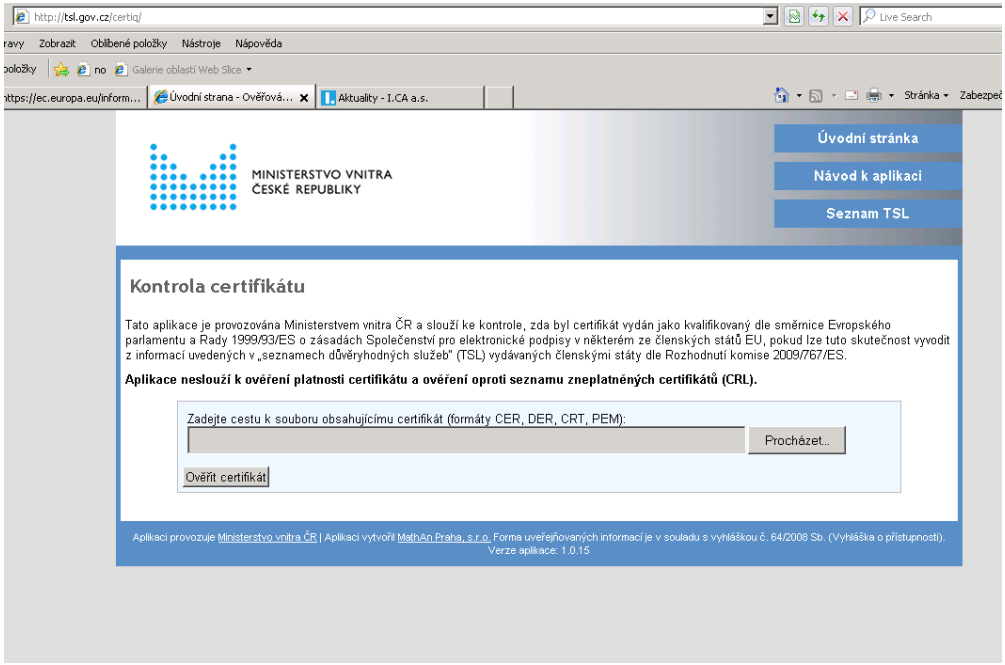
První certifikační autorita a.s. vydala první kvalifikované certifikáty v březnu 2002, Česká pošta s.p. v srpnu 2005 a společnost eIdentity a.s. v prosinci 2005.

3.7. Ověření platnosti certifikátu

První certifikační autorita, a.s. vydala pro Ministerstvo vnitra České republiky certifikát použitý pro bezpečné publikování „důvěryhodných seznamů" (TSL - Trusted Service List). Na stránkách Ministerstva vnitra http://www.mvcr.cz/clanek/verejne-klice-certifikatu-pouzitych-pro-bezpecne-publikovani-duveryhodnych-seznamu-tsl.aspx je ke stažení veřejný klíč certifikátu I.CA, který je používán pro publikování TSL. Tyto seznamy jsou vydávány v souladu s rozhodnutím Komise 2009/767/ES, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst" podle směrnice EP a Rady 2006/123/ES o službách na vnitřním trhu.

U certifikátů je nutné vždy ověřit, zda jde o kvalifikovaný certifikát, protože tuzemští i zahraniční certifikační autority mohou vydávat různé druhy certifikátů. Rozpoznat „kvalifikovanost“ u tuzemského certifikátu je relativně snadné, protože podle naší legislativní úpravy elektronického podpisu musí mít tuto informaci každý kvalifikovaný certifikát v sobě uvedenu. V případě certifikátů od zahraničních vydavatelů je to složitější, a je třeba vycházet z obsahu příslušné certifikační politiky, podle které byl certifikát vydán. Odkazy na tyto politiky jsou sice na seznamech TSL také uvedeny, ale jejich detailní procházení a správná interpretace je již nad možnosti běžného koncového uživatele.

Obr. 3.4: Kontrola certifikátu na stránkách Ministerstva vnitra České republiky



Zdroj: www.mvcr.cz

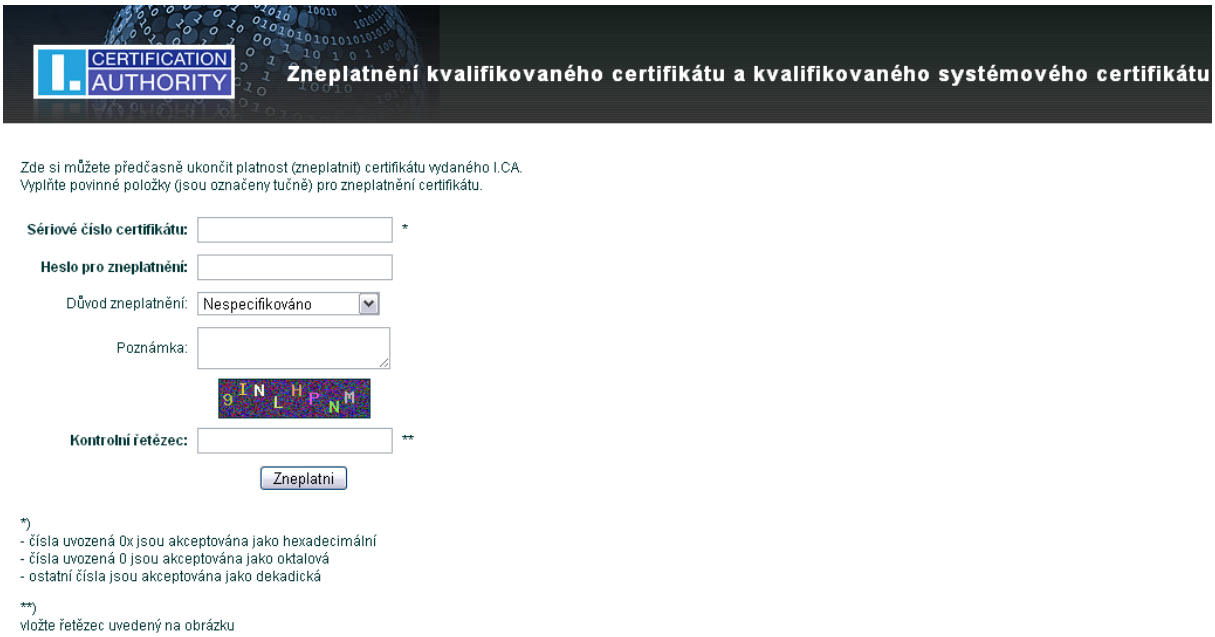
Ministerstvo vnitra ČR, ve snaze vyřešit tento problém, nechalo vytvořit on-line aplikaci, které lze předat konkrétní certifikát, a která na základě seznamů TSL zjistí, zda je možné ho považovat za kvalifikovaný ve smyslu platných zákonů. Jde o aplikaci jménem CertIQ, kterou lze najít na adrese http://TSL.gov.cz/certiq/.Tato aplikace hodnotí pouze to, zda jí předložený certifikát je či není kvalifikovaný. Nehodnotí již další aspekty, konkrétně jeho aktuální platnost. Tu si musí ověřit sám uživatel.

3.8. Zneplatnění certifikátu

V případě potřeby je možné ukončit platnost certifikátu i v době jeho řádné platnosti. Důvodem může být krádež počítače, USB klíče nebo tokenu, na kterém je certifikát uložen. Tato situace je srovnatelná se ztrátou osobních dokladů se všemi důsledky s tím spojenými. Nejzákladnějším způsobem je osobní návštěva. Pokud je třeba zneplatnit certifikát okamžitě mimo pracovní dobu, je toto možné provést pomocí formuláře na webu certifikační autority. Zneplatnění je stvrzeno heslem, které je součástí žádosti o vydání certifikátu.

Odvolaný certifikát je zařazen do seznamu zneplatněných certifikátů (CRL – Certificate revocation list). Na tomto veřejně přístupném seznamu jsou uvedeny neplatné certifikáty, jejich doba platnosti ještě nevypršela. Při každé transakci je tedy možné si prostřednictvím této listiny ověřit platnost daného certifikátu. [7]

Obr. 3.5: Formulář pro zneplatnění certifikátu



Zdroj: http://www.ica.cz/cz/menu/21/prace-s-certifikaty/zadost-o-zneplatneni-certifikatu/

[7] http://www.ica.cz/cz/menu/22/prace-s-certifikaty/seznam-zneplatnenych-certifikatu/

3.9. Obnova certifikátu

Získání certifikátu je poměrně složitá procedura. Znamená kromě generace žádosti o certifikát navíc shromáždění potřebných dokladů, nutných k vydání certifikátu a návštěvu certifikační autority. Tuto proceduru by klienti navíc museli opakovat každý rok po vypršení platnosti certifikátu. Certifikát jako takový se neobnovuje, ale pokaždé se vydává nový.

Řešením pro zjednodušení procedury je požádat o nový certifikát ještě před vypršením platnosti původního a svůj platný kvalifikovaný podpis použít při získání nového certifikátu, který je tímto „obnoven“. V praxi je klient 21 a 7 dní před vypršením platnosti certifikátu na tuto skutečnost svojí certifikační autoritou upozorněn. Při této „obnově“ certifikátu nelze použít žádost z prvotního certifikátu, protože CA požaduje nový pár klíčů. Nově vytvořená žádost o následný certifikát je podepsána soukromým klíčem spojeným s dosud platným prvotním certifikátem. Takto podepsaný dokument je elektronickou poštou odeslán na CA, kde je zpracován. CA po ověření elektronického podpisu na zprávě, celkové kontrole žádost a formálních náležitostí vydá nový certifikát.

4. Elektronický podpis v hospodářské praxi

Při volbě certifikační autority je rozhodující nejen cena certifikátu, ale i dostupnost pobočky certifikační autority, protože pro ověření totožnosti je nutné se osobně dostavit na pobočku certifikační autority. První certifikační autorita a.s. má své pobočky v krajských městech, eIdentity a.s. pouze v Praze. Česká pošta, s.p. poskytuje služby certifikační autority na svých pobočkách, na kterých je dostupná služba Czech POINT.

4.1. Postup při získání a instalace certifikátu PostSignum

Získání certifikátu probíhá v následujících krocích:

- generování páru klíčů,
- doprava žádosti k registrační autoritě,
- ověření žádosti na registrační autoritě,
- ověření informací,
- tvorba certifikátu,
- instalace certifikátu.

Následující kopie obrazovek zobrazují postup při získání certifikátu PostSignum, ostatní certifikační autority umožňují on-line získání certifikátu obdobným způsobem.

Ještě před započetím generování certifikátu je třeba si zvolit vhodné úložiště certifikátu. Rozhodujícím kritériem při volbě úložiště pro zajištění bezpečnosti soukromého klíče je zhodnocení míry rizika zcizení soukromého klíče. Uložení klíče na lokální disk je nejjednodušší metodou. Nevýhodou je, že data z lokálního disku lze poměrně snadno odcizit. V sítích Windows je na disku uložený soukromý klíč součástí uživatelského profilu. Tyto uživatelské profily jsou často konfigurovány tak, že „cestují“ společně s uživatelem a uloží se na každý počítač, ze kterého se uživatel přihlásí do domény Windows. V tomto případě, je tedy riziko zcizení soukromého klíče velmi vysoké a tato možnost uložení soukromého klíče je neakceptovatelná.

Jinou výrazně bezpečnější formou uložení soukromého klíče je hardwarový klíč ve formě čipové karty nebo tokenu. Hardwarový klíč je propojen s počítačem příslušným rozhraním, což může být sériový port, USB, PCI, PCMCIA apod. viz [2]

Nejčastějším druhem hardwarového klíče je čipová karta. Čipová karta je plastová karta, která má ve svém těle vložen čip. Čip je buď vložen do vyfrézované dutiny, nebo v případě bezkontaktních karet se čip zalévá včetně antény přímo do karty. Karta má velikost běžné platební karty nebo SIM

karty mobilního telefonu. Rozměr kontaktů obou karet je shodný a malá karta vzniká vyříznutím z velké. Na trhu jsou i redukce, do kterých lze malou kartu vložit.

Obdobnou technologii jako čtečky používá USB token. Na rozdíl od čipové karty nepotřebuje čtečku a k počítači se připojuje pomocí USB portu. Výhoda tokenu spočívá v tom, že jednou vygenerovaný klíč uvnitř tokenu ho nikdy neopustí. Navíc je token chráněn bezpečnostním PINem.

Obr. 4.1: USB token[8]

V případě, že bylo vybráno úložiště certifikátů, je dalším krokem k získání certifikátu generování páru klíčů a vytvoření žádost o certifikát. Certifikát PostSignum je možné získat on-line za těchto podmínek:

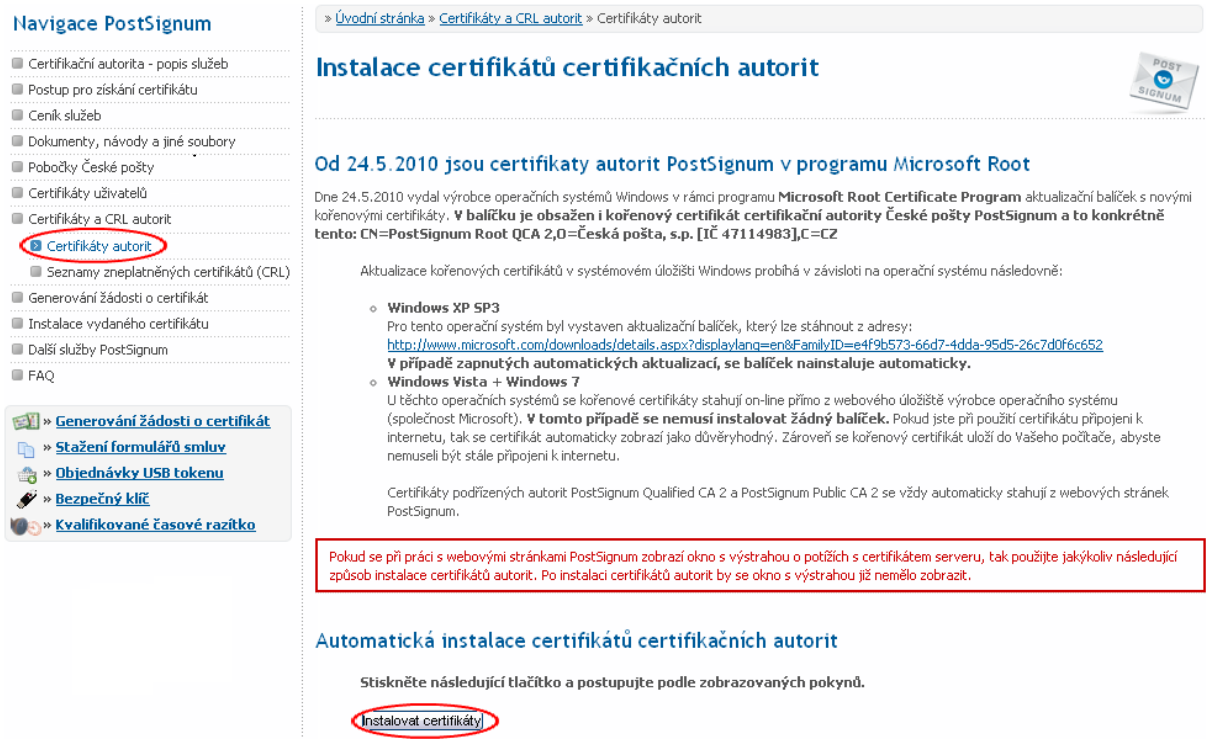
- Používáte operační systém Windows,
- Jako internetový prohlížeč používáte Internet Explorer,
- Máte nainstalovány certifikáty autorit PostSignum.

Většina uživatelů používá operační systém Windows a první podmínka generování on-line způsobem je splněna. Generování je funkční pouze v prostředí internetového prohlížeče IE, žádný jiný prohlížeč generování neumožňuje. Off-line způsob generování žádosti je možný. Uživatel v takovém případě vygeneruje žádost a klíče na USB klíč a při ověřování totožnosti jej předloží.

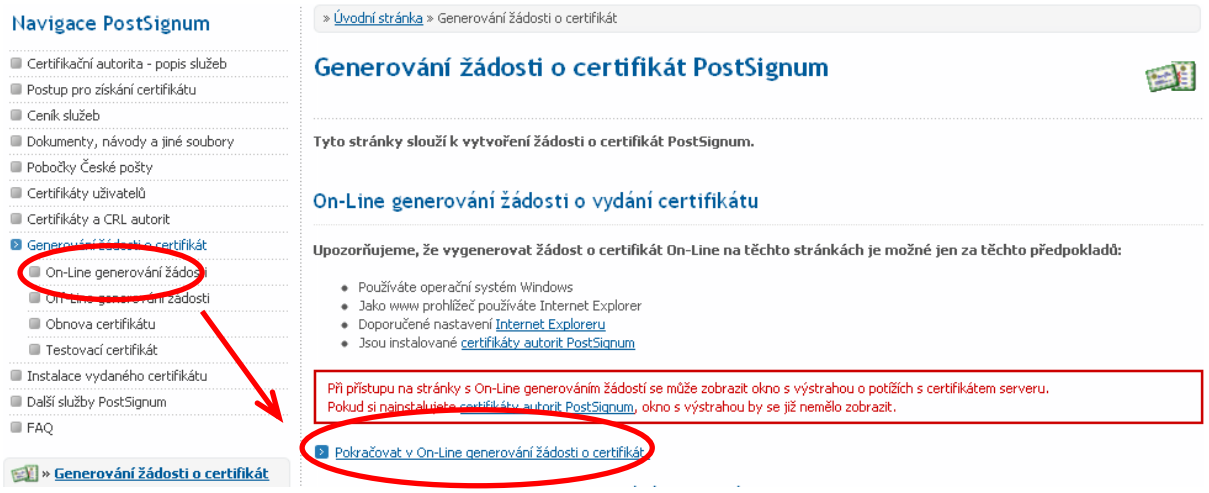
[8] http://www.safenet-inc.com/products/data-protection/two-factor-authentication/ikey-usb-4000/

Po otevření IE prohlížeče je tedy možné přistoupit k samotné instalaci certifikátů certifikačních autorit.

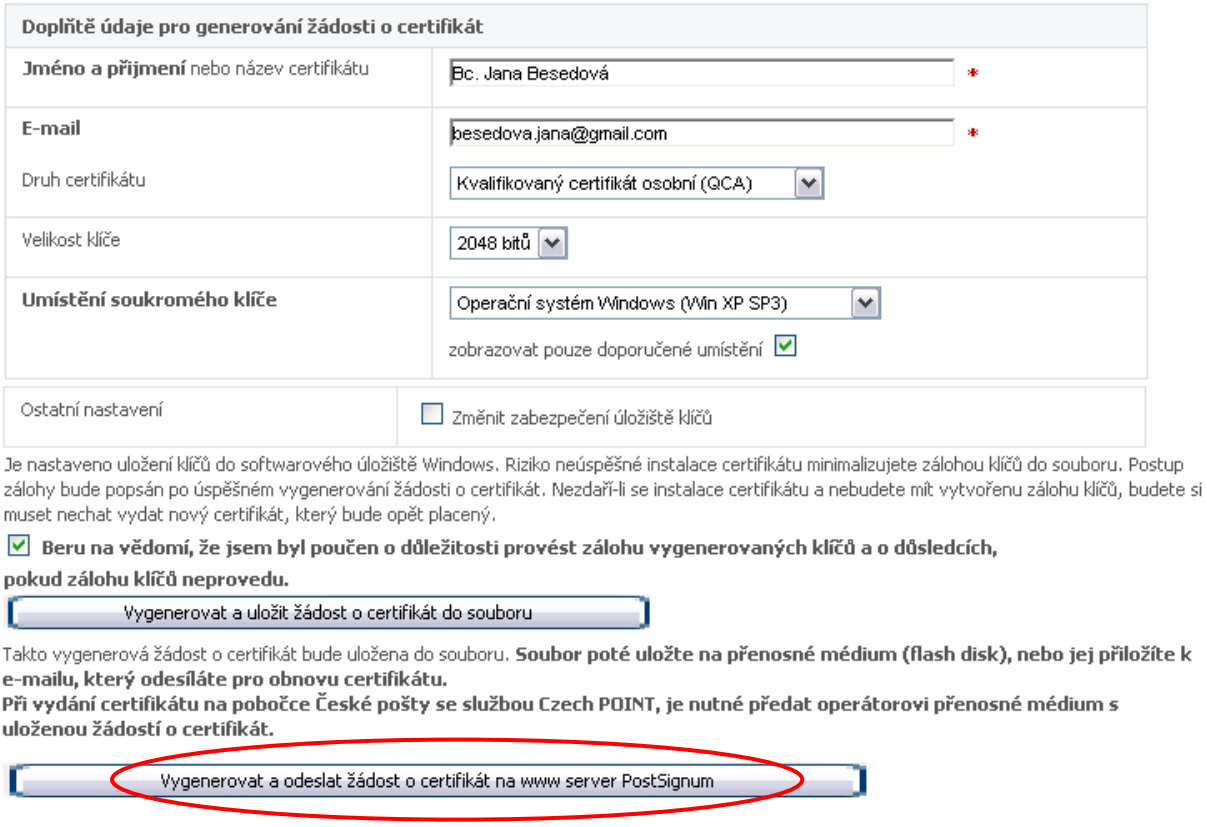
Obr. 4.2: Instalace certifikátů certifikačních autorit



Obr. 4.3: Generování žádosti krok 1



Obr. 4.4: Generování žádosti krok 2



Po vygenerování žádosti je vhodné provést zálohu soukromého klíče. Tato záloha se provede spuštěním v nabídce Start/Spustit programu certmgr.msc, který se zapíše do pole Otevřít. Po otevření pole Certifikáty a otevření složky Požadavek na zápis certifikátu je možné soukromý certifikát exportovat. Přístup k exportovanému certifikátu je chráněn heslem. Vytvořený soubor se zálohou klíčů nesmí získat neoprávněná osoba. Je třeba jej uložit na bezpečné místo, nikomu neposílat ani nepředávat. Tento soubor není potřeba k vydání certifikátu a neposkytuje se České poště.

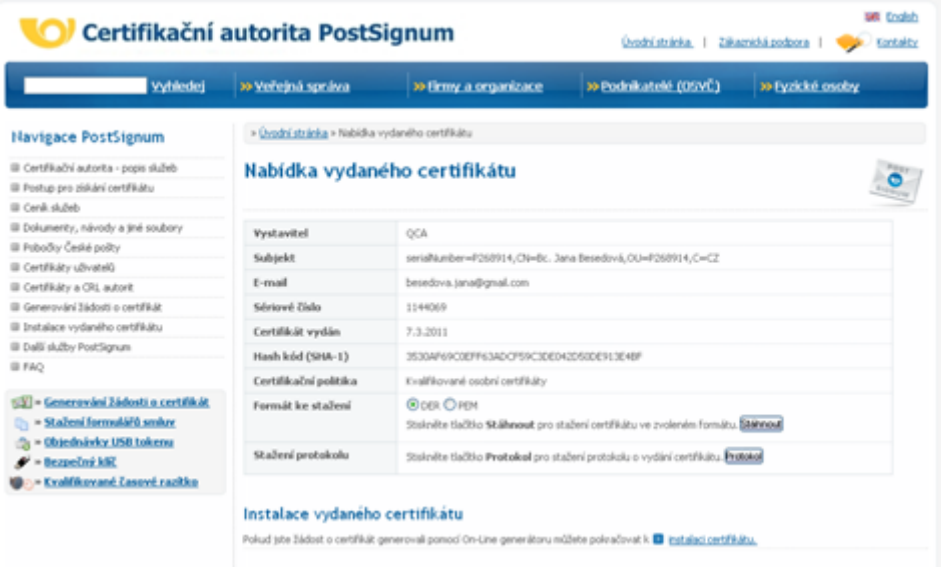
Na pobočku České pošty se službou Czech POINT se musí žadatel o certifikát dostavit osobně. Není možné zplnomocnit svého zástupce nebo provést dálkové vydání certifikátu. Dokumenty potřebné pro ověření:

- vyplněná nepodepsaná smlouva o poskytování certifikačních služeb dostupná na stránkách www.postsignum.cz (2 výtisky Smlouvy o poskytování certifikačních služeb);
- nepodepsané doplněné údaje pro vydání certifikátů (formulář Údaje pro vydávání certifikátů),
- ID žádosti zaslané mailem,
- dva osobní doklady,

- doklad o dosaženém vzdělání, jestliže má být součástí certifikátu titul, který není zapsán v občanském průkazu.

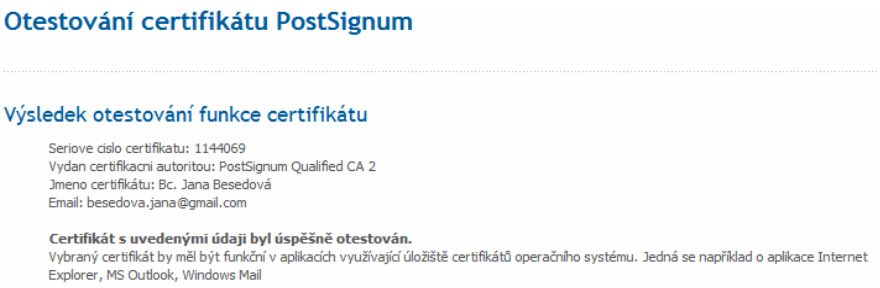
Po ověření žádosti a žadatele, je žádost odeslána pro zpracování. Během dvou dnů je zasláno mailem vyrozumění o připraveném certifikátu s odkazem na adresu, na které je certifikát připraven ke stažení. Celá procedura získání certifikátu není složitá. Stránky poskytovatele PostSignum jsou přehledné a jsou na nich dostupné podrobné návody. Ověření subjektu a zpracování žádosti na pobočce České pošty trvá asi 20 minut. Druhý pracovní den je certifikát zaslán mailem žadateli.

Obr. 4.5: Instalace certifikátu ze zaslaného odkazu



Celý proces instalace je uživatelsky příjemný, intuitivní, pro běžně zkušeného uživatele by měla být instalace bezproblémová. Při instalaci je uživatel vyzván k doinstalování komponenty pro podepisování. Dále je možné provést otestování certifikátu (viz obr. 4.6). Po provedené instalaci certifikátu je možné si jej prohlédnout v internetovém prohlížeči volbou Nástroje/Možnosti internetu/Obsah/Certifikáty (viz Příloha 1).

Obr. 4.6: Otestování funkce certifikátu

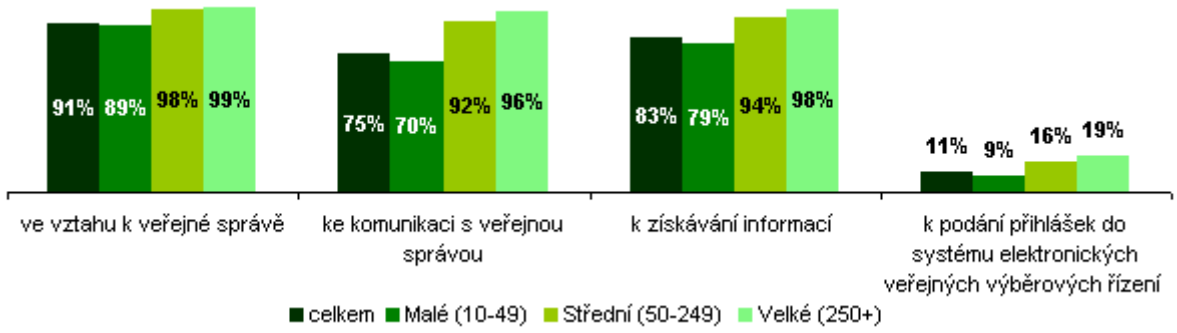


4.2. Využití elektronického podpisu v podnikatelské praxi

Využití elektronické komunikace přináší všem zúčastněným subjektům úspory času, financí, větší komfort při jednání se státem a jeho orgány tím, že se zjednoduší a urychlí komunikace s těmito orgány a zajistí tak větší otevřenost veřejné správy ve vztahu k uživatelům.

V lednu 2010 uvedlo 91 % podniků, že v roce 2009 používalo internet ve vztahu k veřejné správě. Nejvíce používaly internet ve vztahu k veřejné správě podniky z kategorie velké, tzn. podniky mající více jak 250 zaměstnanců, takovýchto podniků bylo 99 %, naopak malých podniků (10-49 zaměstnanců) používalo internet ve vztahu k veřejné správě 89 %. Obecně by se dalo říci, že čím menší jsou podniky, tím menší je jejich zapojení do e-governmentu. Pomocí internetu komunikovalo s veřejnou správou 75 % podniků, tento relativně malý podíl je však způsoben malými podniky, jichž takto komunikuje 70 %. U podniků velkých činil podle posledního šetření jejich podíl 96 %. Nejdynamičtěji rostoucí a zároveň ze sledovaných oblastí nejméně využívanou oblastí e-governmentu je elektronické podávání přihlášek do veřejných výběrových řízení. Stejně jako všechny služby týkající se e-governmentu, tak i elektronické podávání přihlášek je doménou spíše velkých a také středních podniků (50–249 zaměstnanců). V roce 2009 podalo elektronickou přihlášku do veřejných výběrových řízení 19 % velkých, 16 % středních a 9 % malých podniků.[9]

Graf 4.1: Podniky* používající internet ve vztahu k veřejné správě 2009

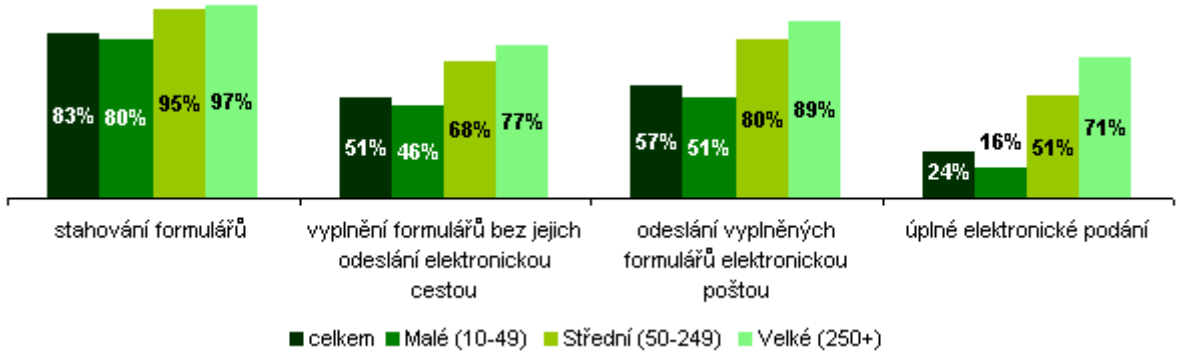


* % podniků v dané velikostní skupině
Zdroj: Český statistický úřad, 2010

[9] http://www.czso.cz/csu/redakce.nsf/i/vyuzivani_ict_ve_vztahu_k_verejne_sprave_podniky

Se zvyšujícím se stupněm interakce dané služby se snižuje podíl podniků tuto službu využívající. Nejčastěji praktikovanou činností na internetu ve vztahu k veřejné správě podniky je tedy prosté využívání internetu k získávání informací z webových stránek úřadů a nejméně pak úplné elektronické podání. Stejně jako v předchozích případech, i zde platí, že čím větší podniky, tím větší je podíl těch, kteří danou službu využívají. Například v roce 2009 vyhledávalo informace na stránkách veřejné správy 98 % velkých a 79 % malých podniků a s použitím elektronického podpisu formulář podalo 71 % velkých a 16 % malých podniků. [10]

Graf 4.2: Podniky používající internet ve vztahu k veřejné správě 2009

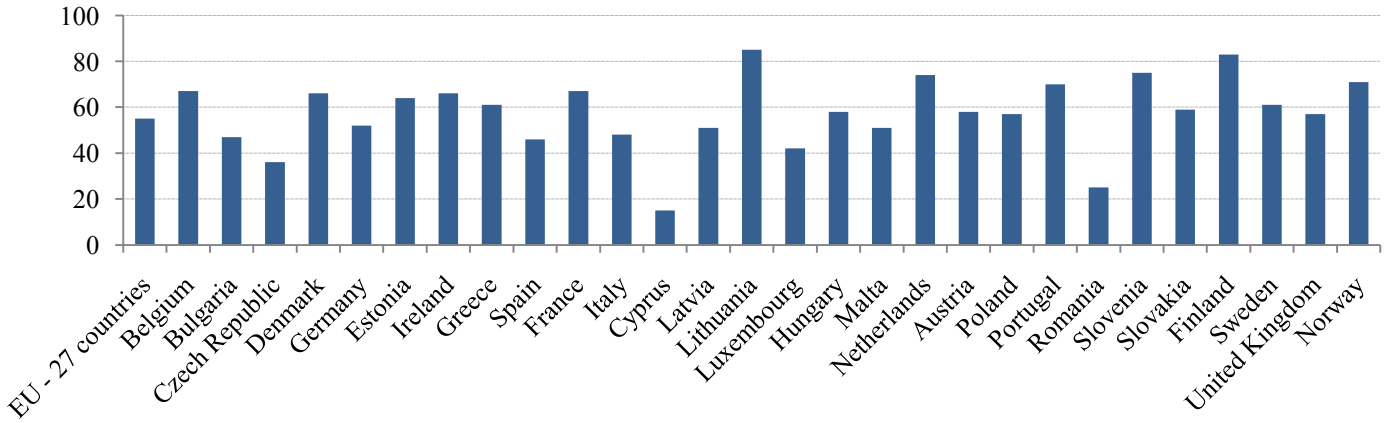


* % podniků v dané velikostní skupině

Zdroj: Český statistický úřad, 2010

V celoevropském měřítku je Česká republika mezi zeměmi, které využívají úplné elektronické podání nejméně. Hůře je na tom pouze Rumunsko s 25 % a Kypr s 15 % úplných elektronických podání z celkového počtu podání veřejné správě. [11]

Graf 4.3: Úplná elektronická podání v Evropské unii v roce 2009



[10] http://www.czso.cz/csu/redakce.nsf/i/vyuzivani_ict_ve_vztahu_k_verejne_sprave_podniky

[11] www.eurostat.com

4.2.1. Datová schránka

Zákon 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů je legislativním základem pro informační systém datových schránek a je účinný od 1. 7. 2009. Informační systém datových schránek je novým komunikačním systémem mezi orgány veřejné moci a právnickými osobami, mezi orgány veřejné moci a podnikajícími fyzickými osobami, orgány veřejné moci a fyzickými osobami a také mezi orgány veřejné moci navzájem.

Od 1. 1. 2010 je navíc umožněna komunikace mezi právnickými osobami, podnikajícími fyzickými osobami a fyzickými osobami navzájem a od uvedeného data je možné dodávat do datových schránek faktury nebo obdobné žádosti o zaplacení, od 1. 7. 2010 je možné dodávat dokumenty libovolného obsahu. Informační systém datových schránek je systém rychlý (datová zpráva je doručena prakticky okamžitě), spolehlivý (datová zpráva se nemůže ztratit), auditovatelný (je jednoduše dokazatelné, kdo datovou zprávu podal a komu byla doručena).

Žádost o zřízení datové schránky se zasílá poštou s ověřeným podpisem žadatele na adresu Ministerstva vnitra České republiky, elektronicky se zaručeným podpisem nebo na kontaktních místech veřejné správy Czech POINT. [12]

Po přihlášení do datové schránky uživatelským jménem a heslem obdrženým poštou se nabízí uživatelům přehledné menu pro výběr jednotlivých činností, které chtějí vykonat.

Obr. 4.7: Úvodní strana datové schránky

[12] http://www.datoveschranky.info

4.2.2. Daňový portál

Daňová informační schránka poskytuje informace z elektronických spisů vedených daňovou správou pro autorizované uživatele. Daňová informační schránka je přístupná na internetových stránkách Daňového portálu Ministerstva vnitra České republiky www.eds.mfcr.cz .

Žádost o zřízení nebo zrušení a žádost k nahlížení do daňové informační schránky lze podat pouze elektronicky, tedy prostřednictvím datové zprávy opatřené zaručeným elektronickým podpisem na předepsaných formulářích. Správce daně o žádosti rozhodne do 15 dnů od obdržení žádosti. Daňový subjekt může k tomuto úkonu zmocnit fyzickou osobu udělením plné moci.

Daňový portál umožňuje uživateli ověřit, zda finanční úřady evidují k určitému datu na osobním daňovém účtu nedoplatek, přeplatek nebo zda jeho stav je vyrovnán. Osobní daňový účet představuje přehled daňových povinností a plateb, které se k nim vztahují. Obsahuje taktéž platby, které je povinen zaslat finanční úřad. Díky tomuto dálkovému přístupu získá poplatník kontrolu nad platbami vůči finančnímu úřadu, aniž by ho musel navštívit.

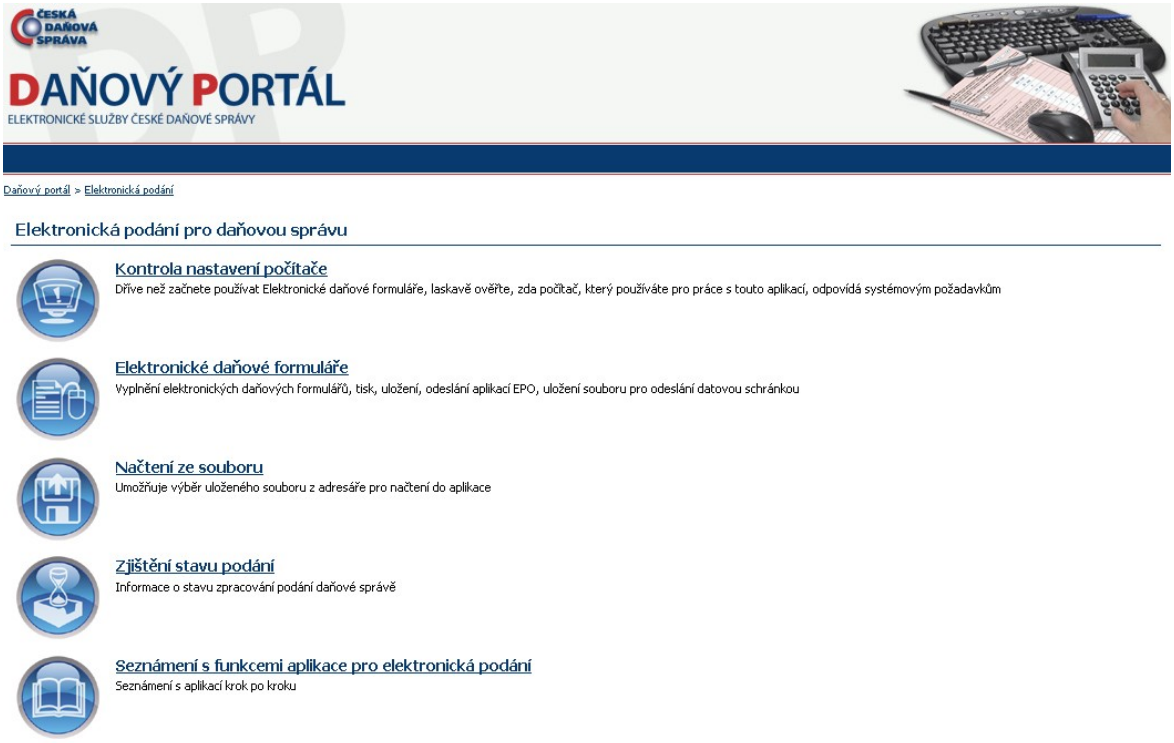
V rámci elektronického podání EPO je možné vytvářet a zpracovávat podání adresovaná daňové správě. Písemnost je možné uložit, zobrazit, uložit nebo i vytisknout v PDF formátu a také elektronicky odeslat s využitím zaručeného elektronického podpisu.

Přehled formulářů, které je možné podat elektronicky prostřednictvím daňového portálu:

- Přiznání k dani z přidané hodnoty platné od 1. 1. 2011,
- Souhrnné hlášení VIES,
- Žádost o přidělení přístupu do Aplikace pro vracení daně z přidané hodnoty plátcům v jiných členských státech,
- Daň z příjmů fyzických osob,
- Daň z příjmů fyzických osob - od roku 2009 včetně,
- Daň z příjmů právnických osob,
- Daň z příjmů právnických osob - pouze pro zdaň. obd. započatá v r. 2010,
- Vyúčtování daně z příjmů ze závislé činnosti včetně všech příloh - za zdaňovací období roku 2010 a pro části zdaňovacího období 2010/2011,
- Žádost podle § 35d odst. 9 zákona o daních z příjmů o poukázání chybějící částky vyplacené plátcem daně poplatníkům na doplatku na daňovém bonusu z ročního zúčtování záloh a daňového zvýhodnění,
- Žádost podle § 35d odst. 5 zákona o daních z příjmů o poukázání chybějící částky vyplacené plátcem daně poplatníkům na měsíčních daňových bonusech,

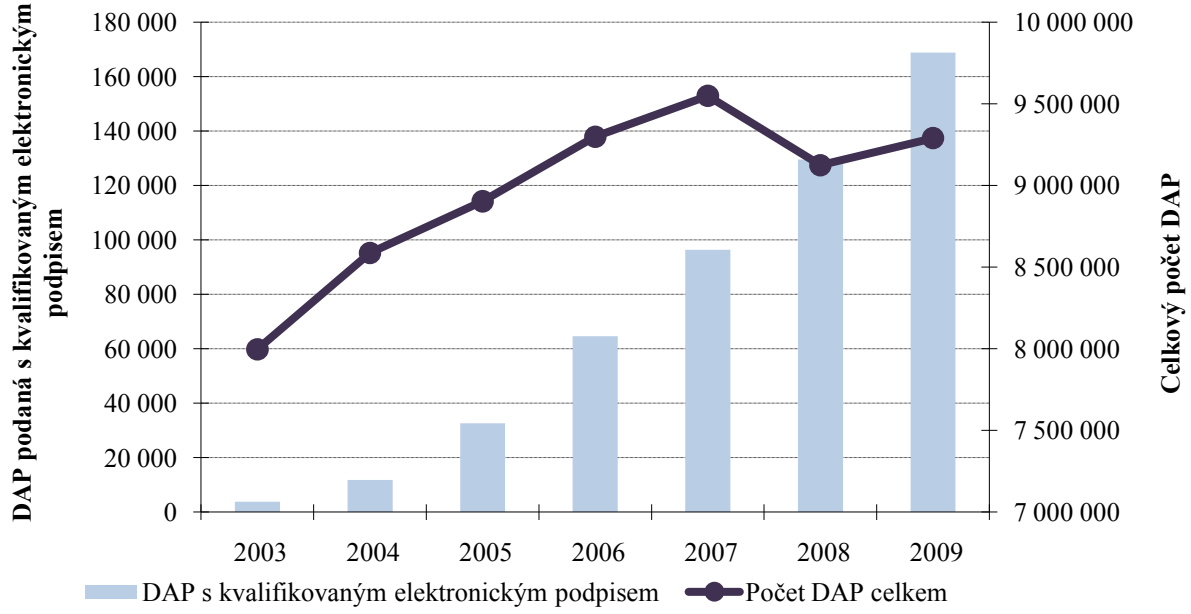
- Vyúčtování daně vybírané srážkou podle zvláštní sazby daně - za zdaňovací období roku 2010 a pro části zdaňovacího období 2010/2011,
- Daňové přiznání k dani silniční - od roku 2009 včetně,
- Daňové přiznání k dani z nemovitostí - od roku 2011 včetně,
- Obecná písemnost určená pro podání státních orgánů a bank,
- Obecná písemnost určená pro finanční úřad, finanční ředitelství nebo Generální finanční ředitelství,
- Oznámení platebního zprostředkovatele podle § 38fa zákona 586/1992 Sb.,
- Žádost o zřízení daňové informační schránky,
- Žádost o zrušení daňové informační schránky,
- Plná moc neomezená,
- Přihláška k nahlížení do daňové informační schránky,
- Plná moc. [13]

Obr. 4.8: Daňový portál



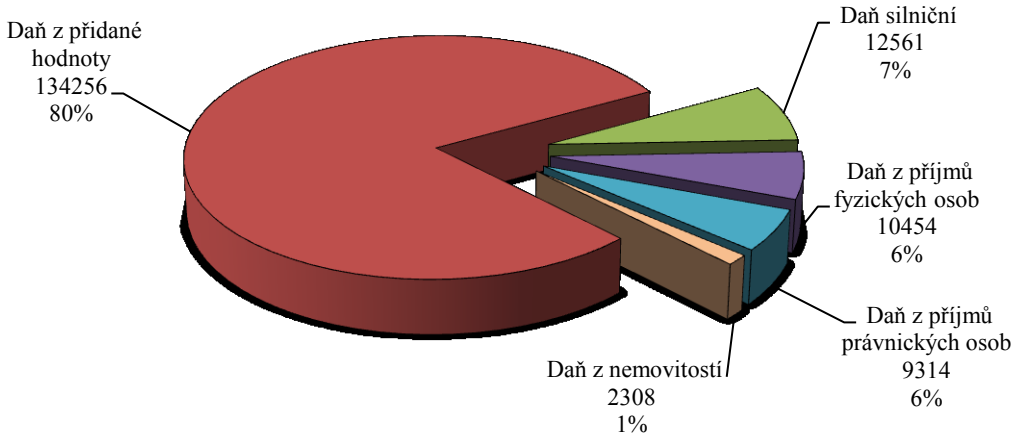
[13] https://adisepo.mfcr.cz/adistc/adis/idpr_epo/epo2/uvod/vstup.faces

Tab. 4.1: Daňová přiznání v České republice v letech 2003 až 2009



Za rok 2009 bylo podáno celkem 9 290 555 daňový přiznání, z toho 188 831 jich bylo v tomto roce podáno jako úplné elektronické podání, což představuje 2,03 %. V roce 2003 činil podíl úplných elektronických podání a celkového počtu podaných daňových přiznání 0,19 %. [14]

Tab. 4.2: Podíl různých typů daňových přiznání podaných s kvalifikovaným elektronickým podpisem za rok 2009



[14] www.mfcr.cz, (detail viz příloha)

4.2.3. Portál veřejné správy

Česká správa sociálního zabezpečení umožňuje klientům zasílat vybrané formuláře elektronicky. Jedná se o tzv. e-Podání, které lze uskutečnit prostřednictvím internetu ve formátu XML. Data jsou předávána České správě sociálního zabezpečení do jejich informačních systémů k dalšímu zpracování. Elektronicky jsou přijímány tyto formuláře:

- Oblast důchodového pojištění
  - Evidenční listy důchodového pojištění
  - Potvrzení o studiu
- Oblast nemocenského pojištění
  - Oznámení o nástupu do zaměstnání
  - Příloha k žádosti o dávku nemocenského pojištění
- Ošetřující lékaři/zdravotnická zařízení
  - Hlášení pracovní neschopnost
- Oblast pojistného na sociální zabezpečení
  - Přehled o výši pojistného (a vyplacených dávkách)
- Osoby samostatně výdělečně činné
  - Přehled o příjmech a výdajích OSVČ

E - podání pro ČSSZ jsou z důvodů bezpečnosti přenosu šifrována. V případě šifrování dokumentu dochází k zašifrování informace pomocí veřejného klíče, který je součástí šifrovacího certifikátu. Dešifrovat data může pouze příjemce zprávy, tedy pouze ČSSZ. Programy, které provádějí šifrování, vyžadují šifrovací certifikát na určeném místě (v úložišti certifikátů). Pro software 602XLM Filler (který jako jediný podporuje ČSSZ) je šifrovací certifikát uložen v úložišti certifikátů Zprostředkující certifikační úřady (ve stejné složce úložiště certifikátů je uložen certifikát „Podřízené certifikační autority“ a „Certifikát kořenové certifikační autority“ je ve složce úložiště „Důvěryhodné kořenové certifikační úřady“). [15]

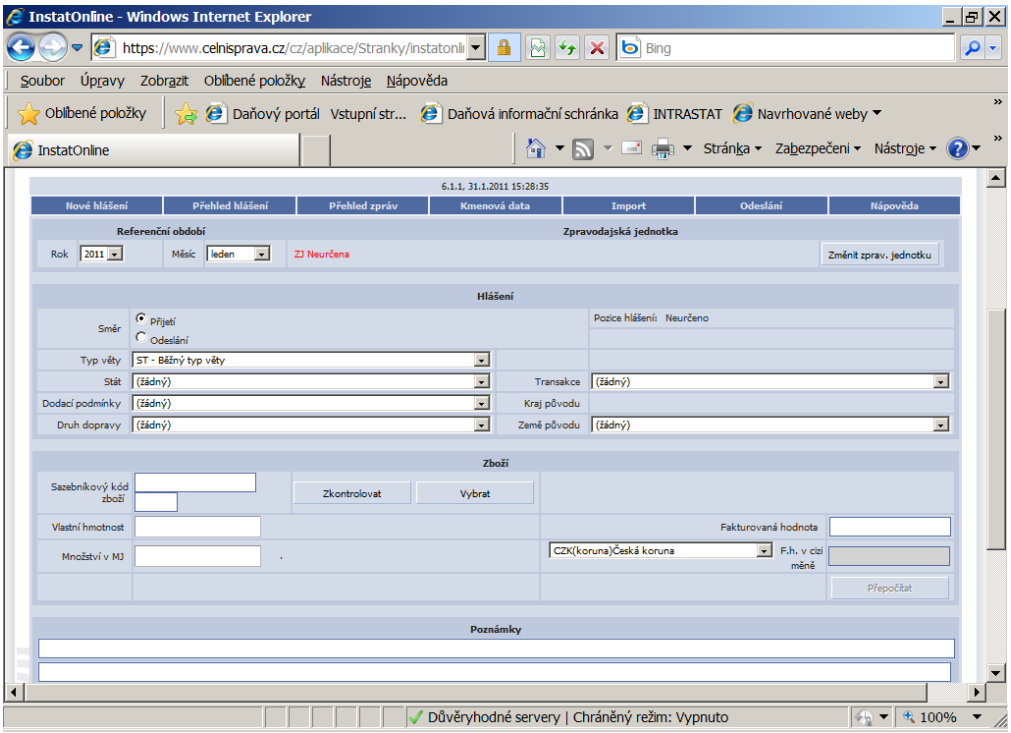
[15] http://www.cssz.cz/cz/e-podani/zakladni-informace/

4.2.4. InstatOnline

Pro usnadnění zpracování dat osobami odpovědnými za poskytování informací dle čl.7 nařízení Evropského parlamentu a Rady č. 638/2004, dle Celního zákona a Vyhlášky 201/2005 Sb. v platném znění, byla Generálním ředitelstvím cel ve spolupráci s Českým statistickým úřadem vyvinuta aplikace InstatOnline, umožňující sběr dat pro statistiku obchodu se zbožím mezi členskými státy Evropské unie. Takto shromážděná data jsou následně zasílána Českému statistickému úřadu.

Aplikace je určena především pro malé a střední firmy. Softwarové požadavky, které má aplikace Instant Online na systém vycházejí z potřeby instalace prohlížeče Microsoft Explorer verze 6.0 a vyšší a v případě elektronického podepisování s nainstalovaným prvkem Active. Data jednotlivých hlášení mohou být zadávána manuálně nebo importována do aplikace InstatOnline z jiných programů. K dispozici je import ve formátu CSV-souboru (Comma Separated Values). InstatOnline obsahuje funkce pro ověření správnosti dat. K dispozici je číselník kódů zboží a řada zobrazení pomocí zadaných filtrů, které usnadňují podání hlášení. Po vyplnění všech polí aplikace je formulář připraven na podepsání kvalifikovaným elektronickým podpisem a odeslání. Po odeslání je možné v aplikaci filtrovat a vyhledávat již odeslaná hlášení, v přehledu jsou jednotlivá hlášení barevně označena podle typu zpráv. [16]

Obr. 4.4: InstatOnline



[16] https://www.celnisprava.cz/cz/Stranky/Login.aspx?ReturnUrl=/cz/aplikace/Stranky/instatonline.aspx

4.2.5. Elektronický podpis e-mailu

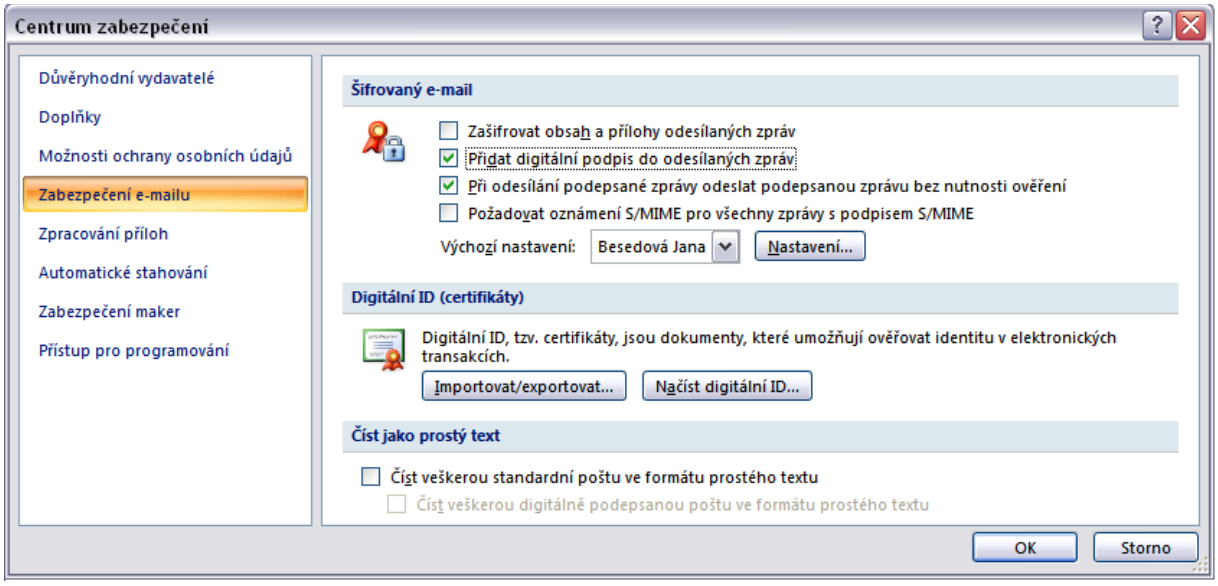
Podpis je symbol, který identifikuje autora. Pro zajištění požadovaného stupně autorizace, autentizace a integrity e-mailu nestačí zprávu pouze slovně podepsat, ale je zapotřebí zvolit sofistikovanější metody.

Elektronické podepsání e-mailu je transparentní proces, při kterém se z celé zprávy včetně příloh vytvoří Hash hodnota. Pokud se do doručení zpráva nezmění (např. i vlivem antivirového programu), potom Hash hodnota souhlasí a podpis je platný. Pro vyhodnocení platnosti podpisu je nutné, aby měl příjemce nainstalované aktuální kořenové certifikáty certifikační autority, certifikát příjemce musí být platný a nesmí být revokován. Organizace příjemce e-mail vyhodnotí při vstupu, zkontroluje platnost podpisu, dokument vytiskne a označí značkou, že podpis byl ověřen a vede se jako ověřený dokument s platným elektronickým podpisem.

Pokud odesílatel nevlastní časové razítko je nutné při komunikaci se státní správou podepsat e-mail a nikoliv pouze samotný dokument. Čas podpisu dokumentu je totiž časem v počítači, se kterým může být manipulováno. Při podepsaném e-mailu orgán státní správy vyhodnotí platnost elektronického podpisu i proti CRL seznamu. Bez časového razítka tedy nelze nikdy v čase vyhodnotit dokument, protože může být podepsán kdykoliv. Pokud orgán státní správy obdrží takový nepodepsaný e-mail, neměl by jej ověřit a neměl by se jím zabývat.

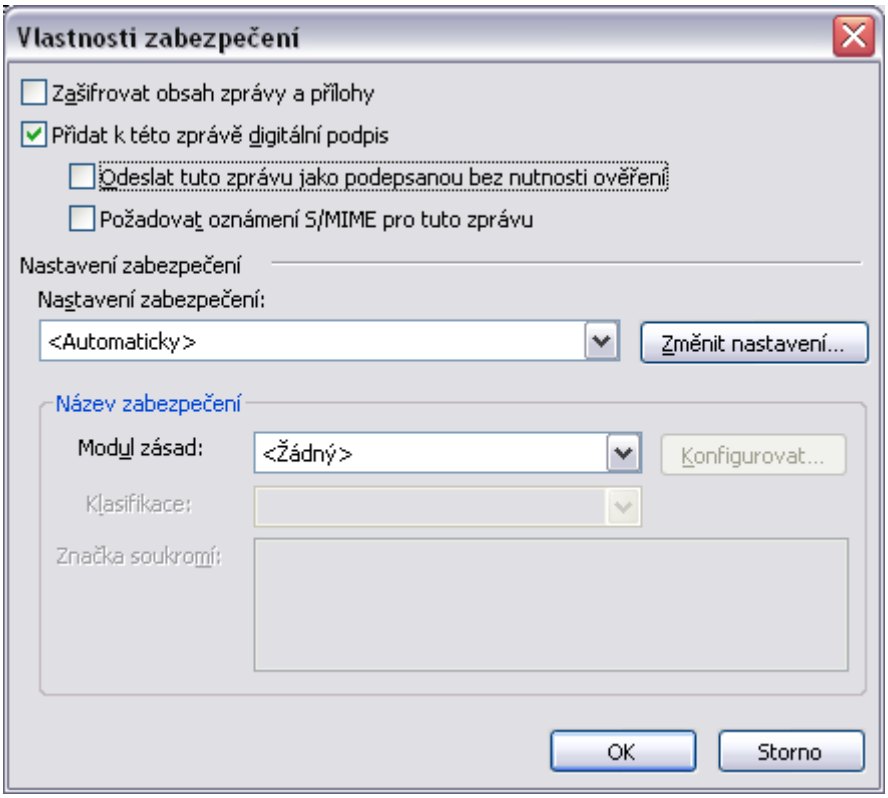
Při použití datové schránky není nutné tento problém řešit, protože identitu odesílatele ověří samotná datová schránka.

Obr. 4.5: Nastavení zabezpečení e-mailu



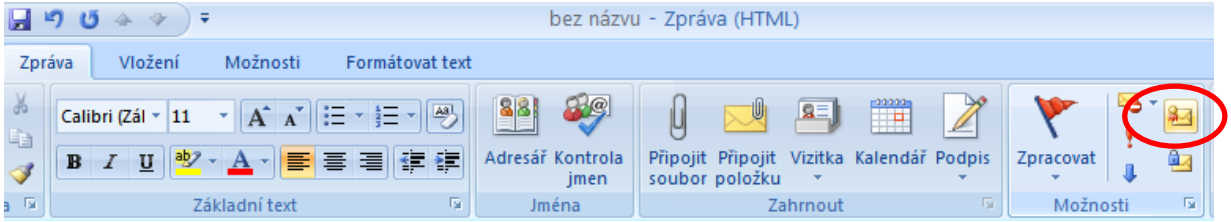
Pro přidání kvalifikovaného elektronického podpisu do e-mailových zpráv v Outlook 2007 je nutné otevřít záložku Nástroje/Centrum zabezpečení/Zabezpečení e-mailu a označit pole Přidat digitální podpis do odesílaných zpráv. Ve volbě nastavení se provádí výběr certifikátu pro podepisování. Po vytvoření nové e-mailové zprávy, se otevře záložka Možnosti a pole Nastavení zabezpečení.

Obr. 4.6: Vlastnosti zabezpečení



Ve vlastnostech zabezpečení se vybírá přidání digitálního podpisu, nutnost ověření a oznámení S/MIME pro tuto vytvořenou zprávu. S/MIME (Secure/Multipurpose Internet Mail Extensions) je současným standardem pro zabezpečení elektronické pošty. Podepsání e-mailu se provede stisknutím tlačítka v nové zprávě.

Obr. 4.7: Podepsání e-mailu



Doručené podepsané zprávy obsahují přílohu smime.p7s. Tento soubor není určen pro otevírání a jedná se o digitální podpis odesílatele. Adresátovi potvrzuje, že e-mail přišel od odesílatele uvedeného v záhlaví e-mailu, a že obsah e-mailu nebyl změněn. Pokud by se tak stalo, poštovní klient příjemce by adresáta varoval, že digitální podpis je neplatný.

4.3. Archivace dokumentů opatřených elektronickým podpisem

Archivace papírových dokumentů je běžnou praxí. V dnešní informační době je většina dokumentů digitalizována nebo se nachází pouze v digitální podobě. Tyto dokumenty je třeba efektivně spravovat a zajistit jejich dostupnost po celou dobu jejich životního cyklu. Archivace digitálních dokumentů je proto nový, dynamický obor, který v současné době ještě není zcela ustálený.

Pro profesionální archivaci digitálních dokumentů jsou nejdůležitější tato hlediska:

- zajištění dostupnosti,
- trvalé organizační a provozní zajištění,
- dlouhodobá stabilita provozovatele,
- zabezpečení ochrany v krizových situacích.

Při dlouhodobém ukládání elektronických dokumentů je třeba se vyrovnat s riziky spojenými s degradací nosičů, zastarání hardware, zastarání formátu, zastarání technologií a ztrátou autenticity, tj. platnosti autentizačních prvků – elektronického podpisu. [17]

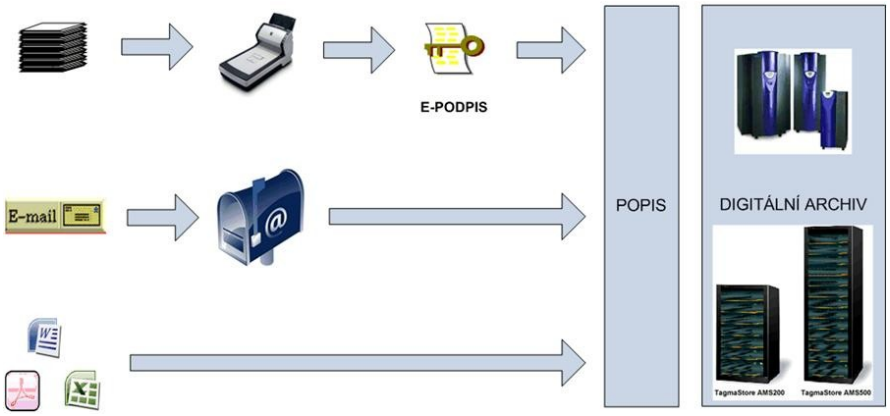
V současné době se jako nejpřijatelnější metoda pro vyrovnání se s riziky dlouhodobé archivace jeví metoda migrace. Metoda je založena na transformaci dat ze staršího formátu do aktuálního. Při této metodě ovšem dochází k narušení integrity dat a ztrátě autentizace. Řešení tohoto problému lze nalézt v užití důvěryhodné instituce, která migraci provede a k dokumentu vydá potvrzení o bezpečnosti. viz [1]

Řešení archivace elektronických dokumentů je horkým tématem roku 2011. Počátkem druhého pololetí 2012 bude ukončena platnost prvních elektronických podpisů, které vznikly při spuštění provozu datových schránek dne 1. 7. 2009.

[17] http://www.cnz.cz/ke-stazeni/2008/konference/prezentace/paces.pdf

To znamená, že firmy, úřady a státní instituce, které budou chtít mít 100 % jistotu platnosti svých dokumentů i v budoucnu, budou muset své prošlé dokumenty pravidelně obnovovat. Do konce roku půjde odhadem až o půl milionu dokumentů. Platnost podpisu, stejně jako v delším horizontu i časového razítka je omezená. Je také zájmem adresáta elektronického dokumentu, aby si dokument udržel svou kvalitu originálu a bylo možno ověřit jeho pravost. V tomto případě je nezbytné u daného dokumentu zajistit pravidelné tzv. "přerazítkování" či využít k podobnému účelu služeb specializovaného poskytovatele důvěryhodného archívu. [18]

Obr. 4.8: Elektronický archív dokumentů



Zdroj: http://www.syconix.cz/cz/elektronicky-archiv-dokumentu

Současná legislativa umožňuje archivovat papírové dokumenty elektronicky při splnění požadavků na elektronickou archivaci. Bohužel zatím v této oblasti neexistuje jednoznačný výklad legislativy, zejména pro případ ověřování dokumentů po vypršení platnosti elektronického podpisu.

4.4. Technologie PDMark[19]

Paper Data Mark je licencovaná technologie společnosti Ardaco a.s. se sídlem v Bratislavě a nabízí uživatelům unikátní možnost sloučení papírového a elektronického dokumentu. Díky této technologii je možné využít výhody elektronických dokumentů, jako je ukládání dat, komprese, šifrování a elektronický podpis, i ve světě papírových dokumentů.

Zápis libovolných dat v digitální podobě na papír s použitím PDMark technologie se realizuje pomocí tiskárny. Binární data se zapisují na papír ve formě drobných čárek.

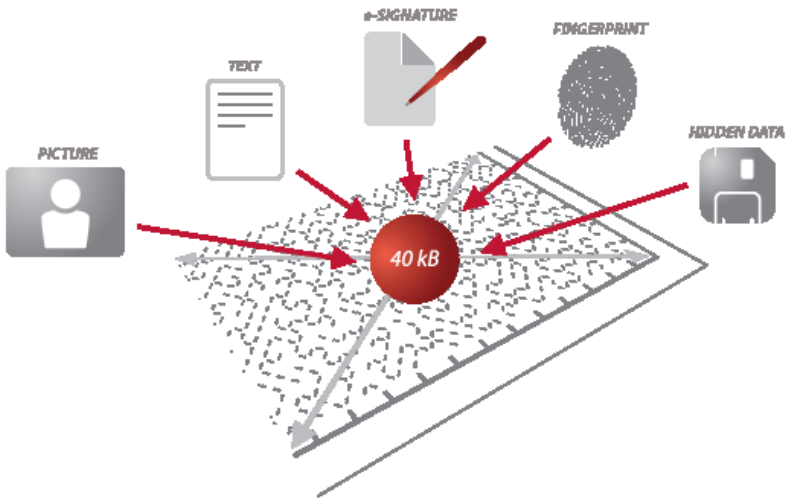
[18] http://www.itpoint.cz/zprava/?i=o2-duveryhodny-archiv-zajistuje-dlouhodobe-pravni-jistoty-elektronicky-podepsanych-dokumentu-6628
[19] www.ardaco.cz

Proces zpětného načtení dat je obdobný jako při načítaní dat z CD disku. Zapsaná data ve formě drobných značek se dekódují a přemění nazpět do původní digitální podoby. Digitální data zapsaná na papír pomocí PDMark se načítají nazpět do počítače pomocí běžného skeneru. Unikátní vlastností technologie PDMark je její schopnost spolehlivě načítat uložená data i navzdory tomu, že byl přes ně vytištěn text či grafika. Jinak řečeno digitální data je možné překrýt viditelným textem či obrázky. PDMark tak například umožňuje uložit na papír digitální soubor s textem současně s jeho viditelnou vytištěnou podobou.

Data se zapisují do pozadí dokumentu, buď na jeho celou plochu nebo do vyhrazené části. Kapacita jednoho listu papíru formátu A4 je přibližně 40-50 kB což představuje například 10 stran textu ve formátu doc. PDMark je schopen zrekonstruovat původní uložený obsah i z výrazně poškozeného dokumentu. Schopnost obnovit původní text záleží na rozsahu poškození originálu a na množství ukládaných dat do pozadí na jeden papír. Technologie PDMark je schopná se úspěšně vypořádat i s poškozeními typu - popsaný, počmáraný dokument, se skvrnami, fyzicky neúplný dokument s odtrženou částí, namočený a vysušený dokument. [20]

Tato technologie představuje přechod mezi papírovým a elektronickým dokumentem. Na Slovensku, které má přísnější režim využívání zaručeného elektronického podpisu a zároveň i propracovanější legislativu týkající se této oblasti, je již technologii využívána ve státní správě a digitální informací založené na této technologii jsou opatřeny výpisy z rejstříku trestů. Informace jsou kódovány do celého dokumentu a působí jako šedý podklad. Neviditelnost ochranného znaku je jeho velkou výhodou, protože není možné falšovat něco, co není pouhým okem vidět.

Obr. 4.9: Technologie PDMark



[20] http://www.e-signature.cz/cs/sprava-dokumentu/paper-data-mark/pdmark-vlastnosti/

4.5. Průzkum využití elektronického podpisu a spokojenosti s portály veřejné správy

METODOLOGIE

Název šetření:	Využití elektronického podpisu v praxi
Předmět šetření:	Rozšíření a využívání elektronického podpisu v podnikatelském sektoru, využívání a spokojenost s aplikacemi e-governmentu
Charakter zjišťovaných ukazatelů:	Kvalitativní otázky (ano-ne): zjištění faktického stavu věcí Subjektivní hodnocení spokojenosti Vyjádření souhlasu/nesouhlasu s výrokem
Cílová populace:	Fyzické osoby zodpovědné za komunikaci firem se státní správou, OSVČ
Technika šetření:	Dotazník rozeslaný e-mailem s použitím webové aplikace stránek www.vyplnto.cz[21]
Způsob výběru jednotek:	Kombinace plošného a záměrného náhodného výběru
Počet zúčastněných jednotek:	60

Sledované ukazatele:

1.	Využití e-governmentu
2.	Vlastnictví kvalifikovaného elektronického podpisu
3.	Spokojenost s portály veřejné správy

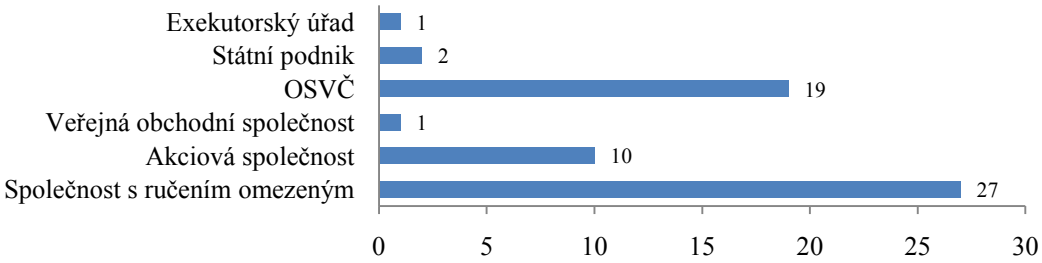
[21] http://vyuziti-elektronickeho-podpi.vyplnto.cz

4.5.1. Informace o respondentech

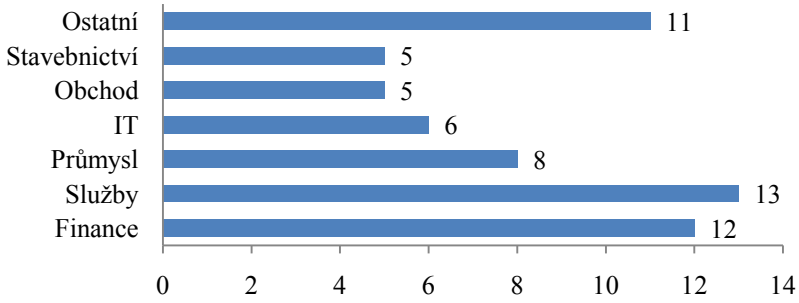
Nabídku na vyplnění dotazníku, který byl zaměřen na využití elektronického podpisu, využití portálů státní správy a spokojenosti s těmito portály, obdrželi respondenti e-mailem nebo informaci o dotazování získali na profesních fórech, např. na webech www.ucetnisvet.cz, www.lupa.cz. Návratnost dotazníku byla přibližně desetiprocentní.

Výzkumu se zúčastnilo celkem 60 respondentů, z toho 47 respondentů bylo osobami zodpovědnými za komunikaci se státní správou. Následující grafy zobrazují strukturu právní formy, předmětu podnikání a počtu zaměstnanců firem respondentů.

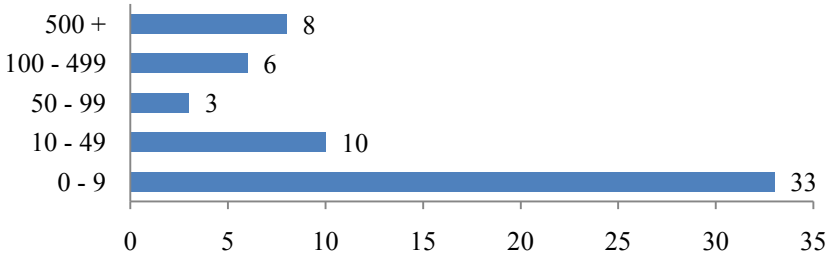
Graf 4.3: Právní forma společnosti



Graf 4.4: Převažující předmět podnikání



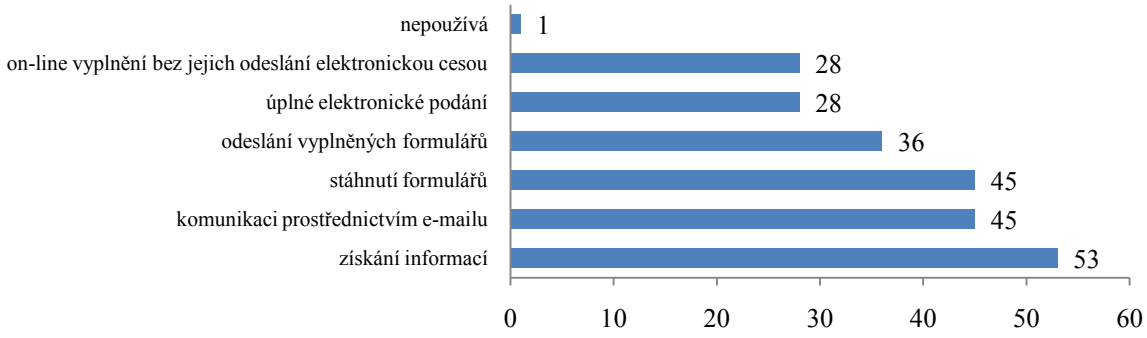
Graf 4.5: Počet zaměstnanců



4.5.2. Využití e-governmentu

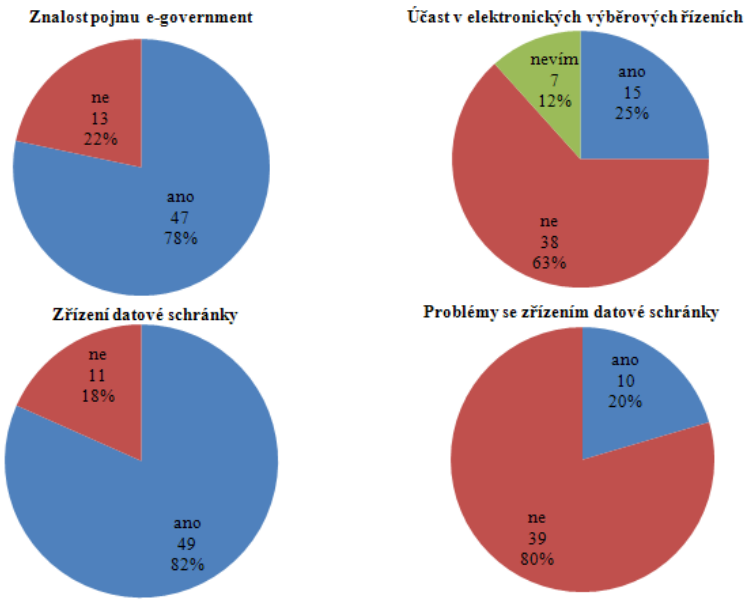
Respondenti byli dotázáni, zda se už setkali s pojmem e-government a více než 78 % odpovědělo kladně. Respondenti rovněž mohli seřadit parametry práce ve webových aplikacích podle důležitosti, kterou jim přikládají. Jako nejdůležitější respondenti uvádějí celkový přínos aplikace, dále její funkčnost, náročnost obsluhy, přehlednost. Na posledním místě se umístil vzhled aplikace.

Graf 4.6: Využití internetu ve vztahu ke státní správě



Se zvyšujícím se stupněm interakce, klesá podíl podniků využívajících tuto službu. Nejvíce využívané je tak prosté získání informací a mezi nejméně využívané patří úplné elektronické podání. 92,88 % společnosti s více než 100 zaměstnanci vyhledávalo informace na portálech veřejné správy a úplné elektronické podání podalo 64,29 % firem velkých firem. U firem s méně než 10 zaměstnanci jsou tyto údaje nižší, a to 84,85 % a 39,39 %.

Graf 4.7: E-government, datová schránka



4.5.3. Vlastnictví kvalifikovaného elektronického podpisu

Kvalifikovaný elektronický podpis má zřízeno 51,67 % respondentů, což představuje 31 osob. Dvě osoby svůj elektronický podpis nepoužívají. V budoucnu si plánuje elektronický podpis pořídit 20,69 % respondentů. 38,71 % respondentů využívá komerční certifikáty a 9,68 % používá časová razítka. Průměrná doba vlastnictví podpisu je 3 roky, 25 jich bylo pořízeno u České pošty s. p., 6 u První certifikační a.s.

4.5.4. Spokojenost s portály veřejné správy

Zjištění míry využití úplných elektronických podání a spokojenosti uživatelů s portály veřejné správy je hlavním cílem průzkumu. Hodnoceny byly tyto portály:

- Datová schránka https://www.mojedatovaschranka.cz
- Portál daňové správy https://adisspr.mfcr.cz
- Portál veřejné správy https://portal.gov.cz
- Instatonline https://www.celnisprava.cz

Respondenti byli požádáni o hodnocení důležitosti, kterou přikládají vlastnostem používaných webových aplikací na stupnici od 1 do 5, kdy 1 je vlastnost aplikace, které přikládají největší význam (viz Tab. 4.5.4.1).

Tab. 4.3: Seřazení parametrů práce ve webových aplikacích podle důležitosti

Odpověď	Průměrné pořadí	Rozptyl
Přínos	2,183	2,116
Funkčnost	2,217	1,203
Náročnost obsluhy	3,133	1,082
Přehlednost	3,233	1,612
Vzhled	4,233	1,112

Respondenti hodnotí jako nejdůležitější vlastnost přínos, který jim aplikace poskytne, následuje funkčnost, náročnost obsluhy, přehlednost a na posledním místě se umístil vzhled aplikace.

Následující tabulka zobrazuje průměrné hodnocení jednotlivých portálů. Respondenti hodnotili portály na stupnici │-2 │ -1 │ 0 │ 1 │ 2 │. Hodnocení se mohli účastnit pouze respondenti, kteří portály aktivně užívají. V případě datových schránek to bylo 49 respondentů, portál daňové správy užívá aktivně 12 respondentů, portál veřejné správy 13 respondentů a portál InstatOnline užívají pouze 2 z celkového počtu respondentů. Výsledky hodnocení portálu Celní správy InstatOnline byly

vyřazeny vzhledem k malému počtu respondentů. Podrobné výsledky průzkumu jsou uvedeny v příloze.

Tab. 4.4: Hodnocení portálů veřejné správy – aritmetický průměr

Vlastnosti aplikací	Datová schránka		Portál daňové správy		Portál veřejné správy	
	průměr	rozptyl	průměr	rozptyl	průměr	rozptyl
Funkčnost	0,633	1,049	0,917	0,41	0,538	0,556
Náročnost obsluhy	0,347	1,043	1,083	0,41	0,308	1,29
Přehlednost	0,408	0,895	0,417	0,91	0,231	0,947
Přínos	0,449	1,349	1,5	0,917	0,846	1,207
Vzhled	0,184	0,844	0,583	1,243	0,154	1,207
Celkové hodnocení	2,021		4,5		2,077	

Jako nejvíce přínosný hodnotí respondenti portál daňové správy, u kterého také nejvíce oceňují jeho funkčnost a také se jeví respondentům jako nejpřehlednější.

4.5.5. Hodnocení portálů veřejné správy

Výsledky průzkumu jsou do značné míry ovlivněny malým počtem respondentů. Nicméně cílů výzkumu zjistit míru využití e-governmentu a spokojenost uživatelů s portály veřejné správy, bylo dosaženo.

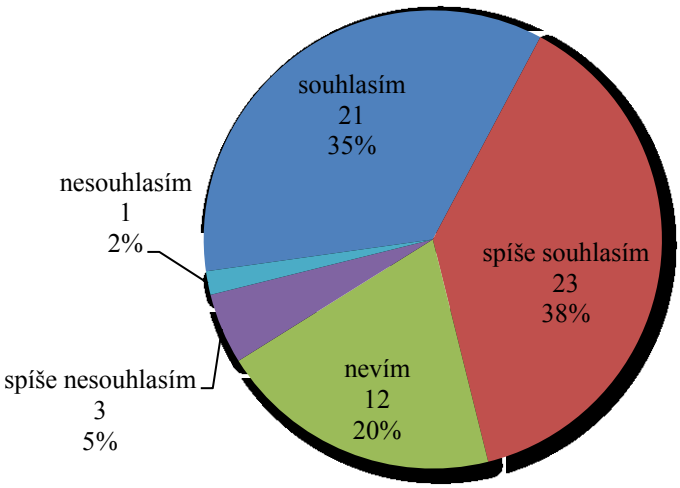
Dotazovaní respondenti nejlépe hodnotí portál daňové správy, který i v komentářích označují jako uživatelsky nejpříjemnější a přínosný pro zpracování a odeslání dat veřejné správě. Nejhůře je hodnocena datová schránka, kterou respondenti označují jako nejméně přínosnou, náročnou na obsluhu a navíc jsou s jejím užíváním spojeny legislativní a provozní problémy. Hlavním problémem, který je zmíněný v připomínkách respondentů (viz příloha), je mazání zpráv po 90 dnech a nutnost zálohovat celou poštu. S úředními dokumenty v elektronické podobě je úzce spjata i konverze dokumentů a vypršení platnosti elektronického podpisu na elektronických dokumentech. Tuto otázku legislativa uspokojivě neřeší a výklad je v současné době značně nejednotný a nejednoznačný.

Portál veřejné správy je hodnocen jako nepřehledný a náročný na obsluhu. Vzhled portálu je hodnocen jako nejslabší z vybraných portálů. Respondenti ovšem oceňují jeho poměrně vysoký přínos, který spočívá hlavně ve značných úsporách času, protože ruční vyplňování formulářů spojených se mzdovou problematikou patří k časově nejnáročnějším činnostem (např. důchodové listy).

Portál Celní správy InstatOnline je moderní a vzhledově propracovaný portál. Práce s portálem je ale časově náročná a zdlouhavá. Většina polí se vyplňuje prostřednictvím rozevíracích

seznamů, žádná opakující položka se neukládá. Příčinou velmi negativního hodnocení vzhledem k tomu, že vzhledu není přikládán velký význam, je nízký komfort práce s portálem.

Obr. 4.10: Celkově hodnotím e-government jako přínosný



Celkové hodnocení e-governmentu je pozitivní. Kladně hodnotilo e-government 73 % respondentů, 20 % se nevyjádřilo a pouze 7 % respondentů jej hodnotilo negativně.

5. Závěr

Problematika týkající se elektronického podpisu je rozsáhlá a jeho větší využití v České republice, spočívající v masovém využití e-governmentu, naráží na mnoho problémů. E-government není prioritou vlády. Ministerstvo informatiky, které by tuto problematiku mělo primárně řešit a bylo zřízeno v roce 2003, bylo zrušeno v roce 2007 a jeho úkoly převzalo Ministerstvo vnitra, Ministerstvo průmyslu a obchodu a Ministerstvo pro místní rozvoj. Důsledkem tohoto roztříštění kompetencí je nedostatečná koordinace, neefektivní využívání prostředků při zavádění informačních technologií a nízký počet služeb e-governmentu. Na nejvyšší úrovni chybí propagátor informační společnosti, neexistuje jednotná vize a pro další zavádění nových služeb e-governmentu není dostatek motivace na všech úrovních státní správy.

Menší podniky nejsou dostatečně informovány o možnostech, které jim e-government nabízí a mezi uživateli panuje nedůvěra k elektronické autorizaci dokumentů a neopodstatněný strach z fatálních následků elektronických podání. Dalším, neméně závažným problémem, je bohužel nedokonalá legislativa. Neexistuje jednoznačný výklad platnosti elektronických dokumentů. Dva názorové proudy na výklad této problematiky jsou v příkrém rozporu. První předpokládá trvalé „přerazítkovávání" elektronických dokumentů v zájmu zajištění nepřetržité platnosti časového razítka i elektronického podpisu. Druhý výklad se opírá o zákon č. 499/2004 Sb. O archivnictví a spisové službě, ve kterém je řečeno, že pokud byl dokument opatřen platným uznávaným podpisem či značkou, má být považován za pravý – a to do té doby, než se prokáže opak. Tato formulace je však specifikem české legislativy a není zřejmé, jak se bude prokazovat platnost takových elektronických dokumentů v zahraničí.

Příslibem pro rozvoj e-governmentu je zřízení Rady vlády pro konkurenceschopnost a informační společnost v březnu 2011. Radě předsedá předseda vlády České republiky a vytyčila si za cíl zavádění informačních a komunikačních technologií a elektronizaci veřejné správy. Rada zpracovává návrhy dlouhodobých a střednědobých koncepcí, analýz, výhledu a směrů, hodnotí nové poznatky a předkládá návrhy jejich možného využití. Tento orgán vlády snad přispěje k rozvoji informační společnosti v České republice a v blízké budoucnosti se podaří vyrovnat se v oblasti e-governmentu ostatním zemím Evropské unie.

Rozvoj informační společnosti je nezadržitelný a je jen otázkou času, kdy počet podání elektronickou formou převýší počet podání v písemné podobě. Už nyní existuje mnoho dokumentů pouze v datové podobě a doba, kdy běžné papírové dokumenty zmizí z hospodářské praxe, může nastat dříve, než se nyní jeví.

POUŽITÉ ZDROJE

a) Knihy, tištěné publikace

[1] BUDIŠ, P. *Elektronický podpis a jeho aplikace v praxi*: certifikáty a certifikační autority, legislativní rámec elektronického podpisu, praktické aplikace. 1. vyd. Olomouc: ANAG, 2008. 157 s. ISBN 978-80-7263-465-1.

[2] DOSTÁLEK, L.; VOHNOUTOVÁ M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2. vyd. Praha: Computer Press, 2009. 542 s. ISBN 978-80-251-2619-6.

[3] MACKOVÁ, A.; ŠTĚDROŇ, B. *Zákon o elektronických úkonech a autorizované konverzi dokumentů s komentářem: včetně souvisejících zákonů a prováděcích předpisů*. 1. vyd. Praha: Wolters Kluver ČR, 2009. 518 s. ISBN 978-80-7357-472-7.

[4] MATES, P.; SMEJKAL, V. *E-government v českém právu*. 1.vyd. Praha: Linde Praha, 2006. 244 s. ISBN 80-7201-614-8.

b) Elektronické publikace

[5] BUDINA, J. *Je e-podpis platný dokud se neprokáže opak?* [online]. 2009, [cit. 2011-03-31]. Dostupný z WWW:<http://www.isvs.cz/e-podpis-podatelny/je-e-podpis-platny-dokud-se-neprokaze-opak.html>.

[6] CVRČEK, D. *Zákon o elektronickém podpisu* [online]. 2001,[cit. 2011-03-21]. Dostupný z WWW: <http://www.fit.vutbr.cz/~cvrcek/system/zep.pdf>.

[7] JEMELKA, P. *Portál veřejné správy – elektronická podání* [online]. 2007, [cit. 2011-04-02]. Dostupný z WWW: <http://www.isvs.cz/portal-gov-cz/portal-verejne-spravy-elektronicka-podani-7-dil.html>.

[8] KOVÁŘ, D. *Elektronický podpis za pár minut* [online]. 2008, [cit. 2011-04-02]. Dostupný z WWW: <http://www.linuxexpres.cz/praxe/elektronicky-podpis-za-par-minut>.

[9] PAČES, P. *Archivace digitálních dokumentů* [online]. 2008, [cit. 2011-03-12]. Dostupný z WWW: <http://www.cnz.cz/ke-stazeni/2008/konference/prezentace/paces.pdf>.

[10] PETERKA, J. *Báječný svět elektronického podpisu* [online]. 2011, [cit. 2011-03-12]. Dostupný z WWW: <http://www.bajecnysvet.cz>.

[11] PETERKA, J. *Proč elektronické podpisy nejsou věčné?* [online]. 2005, [cit. 2011-03-20]. Dostupný z WWW:<http://www.earchiv.cz/b10/b0510001.php3>.

[12] PETERKA, J. *Aktuální stav a perspektivy elektronického podpisu* [online]. 2009, [cit. 2011-03-20]. Dostupný z WWW: < http://www.nic.cz/files/nic/doc/prezentace/Jiri_Peterka.pdf>.

[13] SALNER, A.; MIŠINA, J. *Stav e-governmentu na Slovensku, príčiny a riešenia* [online]. 2007, [cit. 2011-04-01].
Dostupný z WWW: < http://www.governance.sk/assets/files/publikacie/eGov_sk.pdf>.

[14] SMEJKAL, V. *Elektronický podpis jako nástroj pro zvýšení bezpečnosti informačních systémů* [online]. 2003,[cit. 2011-03-20].
Dostupný z WWW:<http://www.vutium.vutbr.cz/tituly/pdf/info/80-214-2447-8.pdf>.

[15] STWORA, V. *Digitální podpis – proč to nikdo nepoužívá?* [online]. 2010, [cit. 201-04-02].
Dostupný z WWW: <http://www.zvedavec.org/techpor/2010/09/3940-digitalni-podpis-proc-to-nikdo-nepouziva.htm>.

[16] ŠMÍD, V. *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), (komentář)* [online]. 2000, [cit. 2011-03-20]. Dostupný z WWW: <http://www.fi.muni.cz/~smid/zelpod.html>.

CA	Certification Authority	certifikační autorita
CRL	Certificate Revocation List	seznam revokovaných certifikátů
CSV	Comma Separeted Values	hodnoty oddělené čárkami
ČSSZ		Česká správa sociálního zabezpečení
EPO		elektronické podání
EU		Evropská unie
HW	Hardware	
ID	Identification	identifikace
IE	Internet Explorer	
kB	kiloByte	jednotka informace, tisíc bajtů
Kč		Koruna česká
OSN		Organizace spojených národů
OSVČ		osoba samostatně výdělečně činná
PCI	Peripheral Component Interconnect	počítačová sběrnice
PCMCIA	Peripheral Component MicroChannel Interconnect Architecture	rozšiřující slot, karty mohou být měněny za chodu a samy si nastavují parametry
PDMark	Paper Data Mark	licencovaná technologie společnosti Ardaco a.s.
PKI	Public Key Infrastructure	označení infrastruktury správy a distribuce veřejných klíčů z asymetrické kryptografie. PKI umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy bez nutnosti jejich individuální kontroly
QCA	Qualified Certification Authority	kvalifikovaná certifikační autorita
S/MIME	Secure/Multipurpose Internet Mail Extensions	Současný standard pro zabezpečení elektronické pošty

SHA	Secure Hash Algorithm	SHA navrhla organizace NSA (Národní bezpečnostní agentura v USA) a vydal NIST (Národní institut pro standardy v USA) jako americký federální standard (FIPS). SHA je rodina pěti algoritmů: SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512. Poslední čtyři varianty se souhrnně uvádějí jako SHA-2. SHA-1 vytvoří obraz zprávy dlouhý 160 bitů. Čísla u ostatních čtyř algoritmů značí délku výstupního otisku v bitech. SHA se používá u několika různých protokolů a aplikací a pro kontrolu integrity souborů nebo ukládání hesel.
SSCD	Secure Signature Creation Device	prostředek pro bezpečné vytváření elektronického podpisu
SW	Software	
TSL	Trusted Service List	seznam důvěryhodných certifikačních služeb
UNCITRAL	United Nations Commision on International Trade Law	Komise OSN pro mezinárodní obchodní právo
USB	Universal Serial Bus	univerzální sériová sběrnice
XLM	Extensible Markup Language	rozšiřitelný značkovací jazyk

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. autorský zákon, zejména § 35 užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;

- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);

- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové (bakalářské) práci budou zveřejněny v informačním systému VŠB-TUO;

- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;

- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě, dne 26. 4. 2011

…….

Bc. Jana Besedová

Adresa trvalého pobytu:
Pod zámečkem 3353
738 01 Frýdek - Místek